CSI: Evidence Indicators for Targeted Ransomware Attacks – Part I

mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks/

February 12, 2020

For many years now I have been working and teaching in the field of digital forensics, malware analysis and threat intelligence. During one of the classes we always talk about Lockard's exchange principle: "with contact between two items, there will be an exchange". If we translate that to the digital world: "when an adversary breaches a system, they will leave traces of evidence behind". The challenge is often how to discover that evidence in a timely manner to take action and discover what sources are available for detection. The volatile evidence sources must be secured as soon as possible while the non-volatile sources have a lower priority. An example of order of volatility:

Order of Volatility	Artifact	Time to change
Volatile	Memory	Microseconds
Volatile	Running Processes	Seconds
Volatile	Network traffic	Seconds to Minutes
Non-Volatile	Disk	Minutes
Stable	Backup /Log files	Day(s)/Week/Month/etc.

Table 1: Order of Volatility

In this series of two articles, you will see an example we have been observing as a concerning trend over the last couple of months.

In the first stage, companies are infected by some sort of information-stealing malware (Azorult, Dridex, Trickbot), or breached by having a weakly secured RDP server at the edge of the network.

Stage two occurs a few weeks later when the same victim is hit by a targeted ransomware campaign using Ryuk, Bitpaymer or another ransomware family the attacker has access to.

A recent example was covered by the team in this article on Bitpaymer. The adversary executing stage one does not necessarily have to be the same as the actor executing stage two. There are plenty of credentials harvested by Azorult or RDP on underground markets. Below is a screenshot from an advertiser demonstrating the number of Azorult victims (13k) they have made, including the information stolen from them:

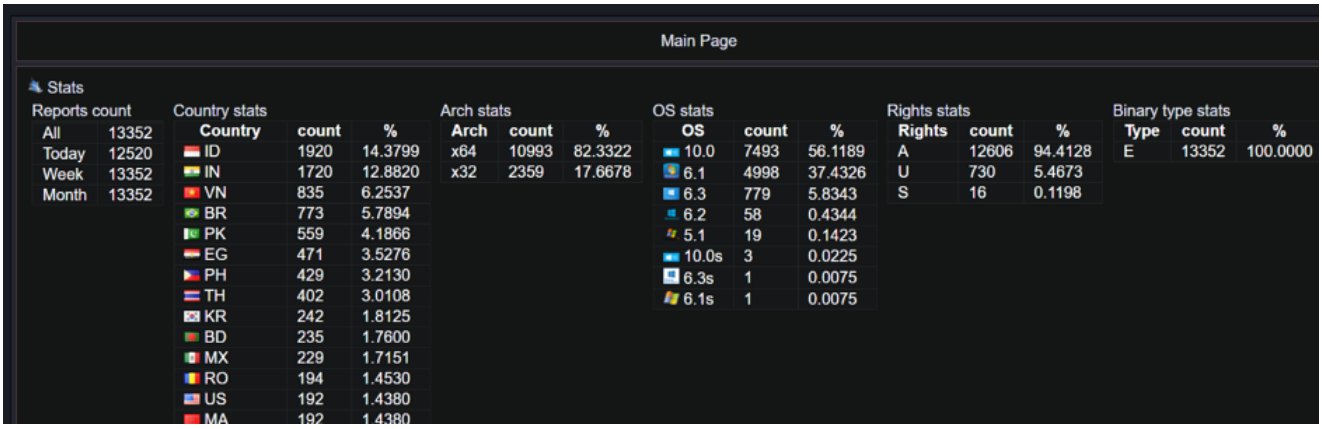

Figure 1 Azorult C2 example

Stage 1: The Initial Infection

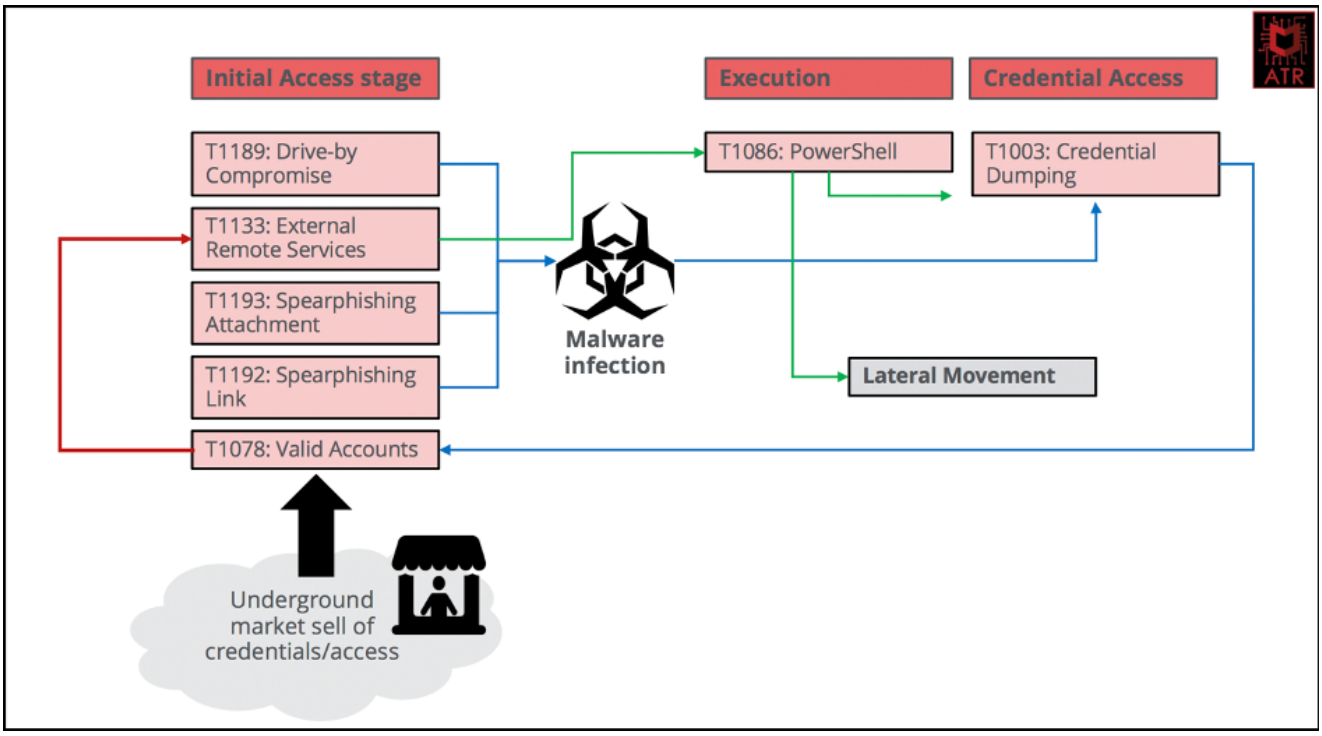

Figure 2 Stage 1

Although there might be some variations, the graphical overview demonstrates how most of these attacks start. Whether by a drive-by compromise where a user visits a website infected with a malicious script or a spear-phishing campaign, the result is a malware infection that steals credentials, exfiltrates them and results in having valid accounts of the victim. The other scenario is buying the valid account information from the underground. Having valid accounts will give access toward a remote service or direct access to a victim's machine using the malware. When an adversary makes the next move, 9 out of 10 times we observe the usage of a credential dumping tool like Mimikatz, or PowerShell related activity again for password dumping. The goal? To get local-admin, domain-admin or system rights on a system within the victim's network. The secondary goal we observe with the usage of PowerShell tools/scripts is conducting reconnaissance of the network.

Digital Evidence Initial Access stage:

T1189 Drive-By Compromise

Order of Volatility	Artifact	Comments
Volatile	Memory	Artifacts can be discovered if memory inspection is ongoing or memory dumped
Volatile	Running Process	Browser process, process launched by script
Volatile	Network traffic	Leaves traces in network-management logs
Non-Volatile	Disk	Browser index files/history/database/cache/cookies/ temp files
Stable	Log files	Network device related logs: Gateway/Firewall

In this scenario the victim most likely browses the Internet and visits a webpage that contains a malicious script. Following the order of Volatility, where could we discover evidence? Depending on what type of actions are defined in the malicious script, it could leave traces on disk or in memory when injected.

T1192 & T1193 Spear-phishing Link/Attachment

In this scenario, the victim receives an email with a link (T1192) or a weaponized attachment (T1193). By clicking on the link, a website is opened, and follow-up actions are executed as described above in the T1189 Drive-by compromise. The order of volatility is similar but will have a larger chain of execution. Since the user initiated the action, more digital evidence will be available on the victim's machine:

1. Execution of a program (Email-client)
2. Clicking on the link will open the default configured Web-browser
3. Web-browser visits link
4. Script will execute

For the execution of a program and launch, there is process evidence, the prefetch directory, UserAssist, Shimcache, RecentApps and many more sources to track when they were launched and executed. The email itself can either be retrieved from the victim's inbox or, in the case of Webmail, there might be remnants of it in the temporary Internet files. Most of the mentioned evidence artifacts are non-volatile and easy to extract in a forensically sound matter.

In the case of a spear-phishing attack with a weaponized attachment, the flow will look mostly similar to below (of course there are variations):

1. Execution of a program (Email-client)
2. Opening attachment
3. Launch of Office application
4. Execution of the macro
5. PowerShell/WMIC followed by Internet traffic downloading file
6. Execution of script/file
7. Execution in memory or written to disk and execution

We already discussed the non-volatile evidence available for the execution of a program. In this example there will be evidence for the launch/execution of the email-client and the opening of an Office application to execute the attachment. In case the attachment was opened before saving to disk, in Outlook the file was copied to the "SecureTemp" folder which is a hidden folder under Temporary Internet files.

Depending on the payload of the macro, evidence will exist of Internet related traffic. When PowerShell or WMIC is used, the launch of it is recorded in the Windows Prefetch directory and there are traces in the registry and/or event logs. Depending on what type of script or file

is executed, traces can be discovered in memory or on disk, with memory most volatile and disk non-volatile.

When, for example, a malware like Azorult is installed on the victim's machine, the flow will look like this:

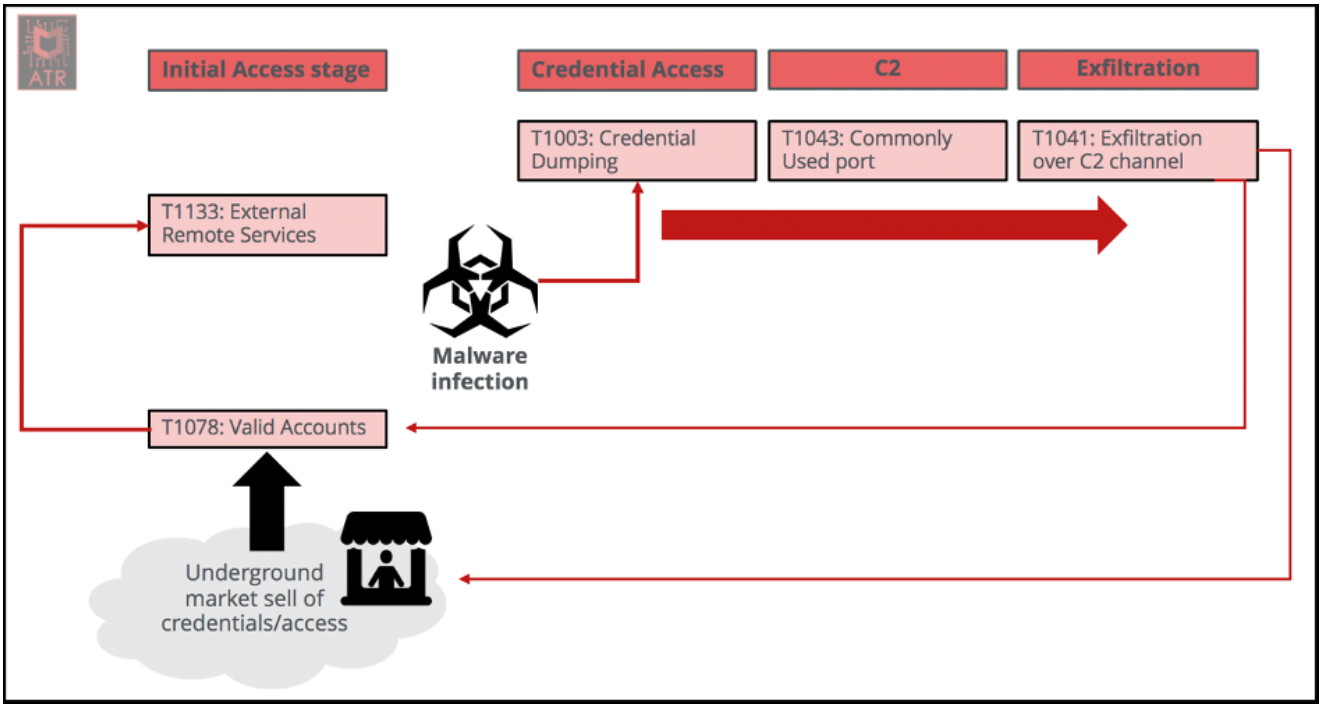

Figure 3 Exfiltration and Communication

The exfiltration of the data is mostly happening over TCP port 80 towards a C2 (command and control) dashboard, as demonstrated in Figure 1. Both T1043 and T1041 are techniques that will most likely leave non-volatile traces behind in network logs from devices like a proxy/gateway/firewall.

What we notice often is that infections with, for example, AZORULT are ignored/underestimated. They are being detected and the infection is either blocked or detected and later cleaned, however the capabilities of the malware are underestimated/ignored.

If we look again to table 1, the order of Volatility, the timeframe in which we operate is seconds to minutes with regards to initial network traffic and running of processes. Between infection and exfiltration is again in the timeframe of minutes, more than enough to exfiltrate credentials before an action was taken. This is also the delta in which we have the challenge – are our people, processes and technology combined capable of responding within this attack-window? Anticipating early warning signs and understanding the malware's capabilities can assist in preventing larger damage.

What happens when the initial compromise results in having valid credentials or victim access through the RAT (random access Trojan), being used for a targeted ransomware attack? We will discuss that in the next article.

Christiaan Beek Lead Scientist & Sr. Principal Engineer

Christiaan Beek is the Lead Scientist & Sr. Principal Engineer of the Enterprise Office of the CTO. He is leading the strategic threat intelligence research with a focus on inventing...