NOW YOU SEE IT, NOW YOU DON'T: WIPERS IN THE WILD

Saher Naumaan
BAE Systems Applied Intelligence, UK

saher.naumaan@baesystems.com

ABSTRACT

Wipers are an APT's new best friend. Traditionally, it is rare for destructive malware to appear in cyber espionage, and it generally runs counter to the conventional interests of an Advanced Persistent Threat (APT) – such as intelligence collection, persistence and covert access. But wiper malware is now appearing more often, emerging in APT toolkits, and was seen in at least four attacks in 2017 following only a handful of instances in the previous decade.

Does this mean the motivations of state actors are changing? We have seen APTs deviate from espionage and branch into criminal operations such as bank heists and the sabotage of critical infrastructure and industrial control systems. From the debilitating WannaCry to the sophisticated false flag Olympic Destroyer, the heightened deployment of wipers suggests there has been an evolution in attacker behaviour.

This paper examines three different classifications of wipers through examples of various politically targeted attacks: *espionage* (in the cases of Flame and StoneDrill), *sabotage* (seen in the cases of Shamoon 2.0 and DarkSeoul) and *diversion* (seen in the cases of Hermes and MBR Killer in bank heists in Taiwan and Chile, respectively). Wipers have become a low-cost way for state actors to conduct destructive attacks that serve multiple purposes – they have significantly more impact on victims and impede investigation into primarily non-destructive attacks.

INTRODUCTION

Traditional state-sponsored hacking activity is often focused around cyber espionage, as the primary interests of an Advanced Persistent Threat (APT) tend to focus on intelligence collection, exfiltration of sensitive data, persistence, and covert access. However, we have also seen APTs deviate from espionage and branch into criminal operations such as bank heists and sabotage through attacks on critical infrastructure and industrial control systems (ICS). The nature of state-sponsored attacks is changing as their motivations and capabilities evolve.

The tools used in offensive cyber operations cover a vast range and include backdoors, remote access trojans (RATs), implants, and even destructive malware. This range also includes wipers, which have existed for years but which have, until now, remained rare in state-sponsored operations. Wipers are discussed in the context of targeted attacks, the scope of which does not include criminal ransomware. The following discussion is also restricted to wiper malware, precluding other destructive malware such as Stuxnet and TRISIS/Triton.

In the last 10 years we have witnessed only a handful of major wiper attacks, but their use has escalated since 2016, from the global and debilitating WannaCry to the most sophisticated false flag to date, Olympic Destroyer. The minimal use of wipers over the last decade and their heightened deployment in recent years suggests there has been an evolution in APT behaviour.

Our case studies of wiper attacks highlight three clear categories of wiper use: espionage, sabotage and diversion. We first look at the use of wipers for espionage – we discuss the usual motivations of state actors, and the incorporation of a new tactic, with reference to the unusual appearance of wiper functionality in intrusions. The case studies presented are Flame and StoneDrill. The next section covers the most commonly associated use of wipers: sabotage. Prominent examples include Shamoon, Shamoon 2.0 and DarkSeoul, all of which had the aim of deliberate system destruction. Finally, 2017 and 2018 have seen the emergence of a new strategy for wiper use – diversion – as demonstrated by Hermes and MBR Killer in the Taiwanese and Chilean bank heists.

This paper argues that wipers have become a routine part of an APT toolkit, though their application isn't limited to destruction. While wiper functionality always results in the destruction of data or systems, this is not always the wiper's sole intent or purpose. This paper evaluates the use of wipers as a new tactic in targeted state-sponsored attacks, looking at several examples, and highlights the significance of this trend.

ANATOMY AND FUNCTION OF A WIPER

Destruction, the function of a wiper, is reflected in its anatomy, which consists of a destructive payload and a propagation mechanism. However, there are nuances and variations in how a wiper is constructed and how it executes.

Payload types

A wiper targets one or a subset of three attack vectors: files, the boot section,[1] and the backup of the system and data.

- The most unmistakable wiper attack is against **files**. For efficiency purposes, most wipers are selective in their wiping and won't overwrite the entire hard disk. Some wipers target files with specific extensions, or folders, and some only rewrite enough bytes in each file to destroy the file headers and prevent them from being opened.
- Another target of wipers can be the **boot section**. Such an attack works either by erasing the first 10 sectors of the physical disks or by overwriting the first 10 sectors with a new boot loader, as in the Shamoon attacks (discussed later). Either way, files aren't just erased – the original operating system becomes unbootable because the Master Boot Record (MBR) section of the hard disk has been corrupted.[2]
- If the goal is complete corruption, the malware must also attack all **backups and shadow copies**. In Duqu, the attackers scrubbed the servers – the files weren't just

[1] Related targets include file tables and partition tables.
[2] Wipers can and have targeted other elements of the physical disks, including NTFS boot sectors and corresponding Master File Tables (MFTs) and their backups. Even if NTFS boot sector corruptions were manually resolved, the lack of the MFT would result in files needing to be carved manually from disk. The files themselves are left intact.

deleted, but the data had been overwritten to prevent restoration [1].

The wiper attacks that targeted the Iranian Oil Ministry and Iranian National Oil Company in April 2012 demonstrated selective and targeted wiping [2]. Most files were wiped with a repetitive pattern that ensured every header was destroyed, yet other parts of the files remained intact. The wiper likely searched for and destroyed files with certain extensions, then targeted all files in certain folders, and finally overwrote the disk sectors. The attackers first wiped the malware components, and only then targeted other files in the system, which eventually made the machine crash.

Infection/propagation

As with other malware, a wiper requires a delivery mechanism. Some malware uses phishing as an infiltration vector, though in the case of a wiper, it would be less common and less advantageous for an attacker because the goal is usually to infect as many boxes as possible. A wiper could also theoretically be pushed to all machines on a network, such as in the case of NotPetya, which compromised victims through a malicious software update of *MEDoc*.

Wiper *worms*, however, consist of a destructive payload *and* a propagation mechanism, which allows the wiper to spread across machines and networks. NotPetya and Olympic Destroyer are examples of wiper worms, meaning they were able to self-propagate – to remotely copy and execute the wiper – and perform lateral movement.

While conventional understanding of wipers assumes their singular purpose is destruction or disruption [3], the following case studies show that functionality is different from intent and purpose. The *function* of all wipers is destruction, but the *intent* behind their destructive capability varies and seems to be evolving.

HISTORY OF WIPERS

Wipers appeared in targeted attacks as early as 2009 with the use of Dozer on South Korean targets as part of the DarkSeoul attacks. In fact, *Talos* has blogged that it has 'historic examples of this type of malware [wipers] going back to the 1990s' [4], referencing variants of the Destover malware that attacked *Sony Pictures* in 2014.

Instances of wiper use, and even destructive operations in general, have been limited over the last ten years compared to other types of intrusions. However, it appears to be an increasingly popular tactic, with seven high-profile destructive attacks occurring in the last three years. In most cases, the ultimate aim is destruction, but other cases, such as examples of Lazarus activity, show that wipers are even being used to remove evidence of their own activity or as a diversion technique.

CLASSIFICATION OF WIPERS

In an exploration of wipers in the context of state-sponsored, targeted attacks, several examples demonstrate the variety and evolution of wiper use cases. We classify them as three distinct use cases.

Espionage

Espionage is 'an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information' [5]. The most strategic use of wipers, espionage is primarily directed at collecting intelligence to serve a higher purpose, rather than as an instrumental goal-oriented operation.

Flame/sKyWIper

One of the older cyber espionage operations, Flame was a large-scale and sophisticated campaign that was active for at least five years before its discovery in 2012 in organizations in the Middle East, primarily Iran.[3] The Flame malware would automatically collect everything from infected machines: keystrokes, audio recordings from the internal microphone, screenshots, documents, and network traffic. The complexity of Flame suggests its purpose was long-term surveillance rather

[3] Flame could date back to as early as 2007, around the time Stuxnet and Duqu were likely created – one component of Flame was seen in December 2007.

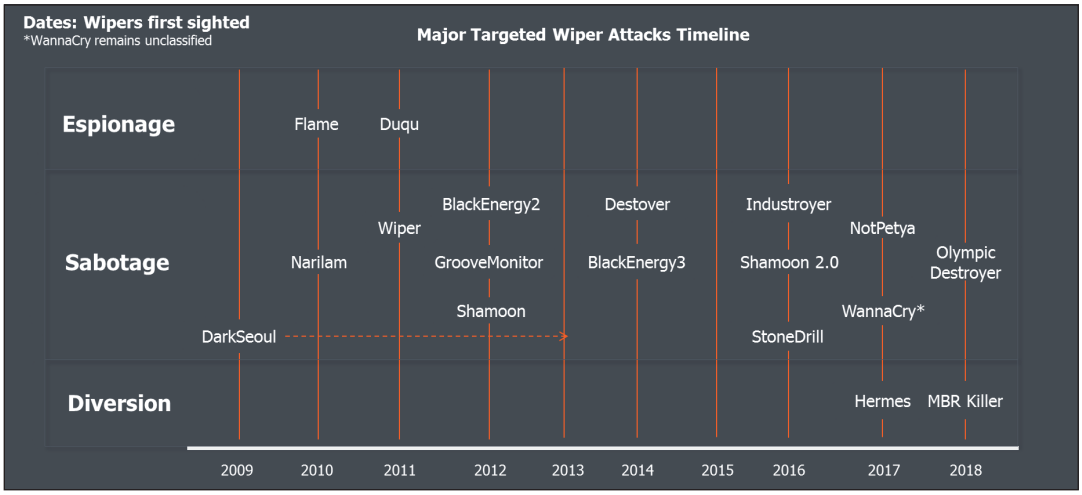

Figure 1: Major targeted attacks employing wipers and classifications.

Figure 2: Flame code.

than short-term sabotage, though the malware also contained a wiper component.

The wiper functionality was in the form of a *Linux* script called 'LogWiper.sh', renamed from 'LogWiper_fixed.txt', which established server environments for the attackers to use as C&C servers [6]. The attackers used a careful approach, ensuring the clean-up of victims' and their own infrastructure. The malware wiped existing log files, securely deleted any prior log files created, and disabled logging in two applications to mask evidence of their activity [7].

At the end of the script the attackers wrote a command to remove the original script using SHREDER – a malware self-removal *Windows* binary file that repeatedly overwrites files to prevent their recovery. The command attempted to delete 'logging.sh', but the current script is called 'LogWiper.sh' so it wasn't deleted.

In June 2012, some Flame C&Cs sent an updated command to some compromised computers. The file, called `browse32.ocx` (the uninstaller), was responsible for removing Flame from the compromised machine [8]. The module locates every file on disk, removes it, and then overwrites the disk with random characters to prevent forensics being done on the machine, leaving no traces of the infection.

Analysed Flame code revealed a component named SUICIDE, which is functionally similar to `browse32.ocx.11` [8]. It remains unknown why the attackers opted not to use the SUICIDE functionality and instead made Flame implement actions from a new module. It is possible that there was a flaw in the SUICIDE module, or it contained an outdated list of files to target.

Sabotage

Sabotage is 'a deliberate attempt to weaken or destroy an economic or military system' [5]. There is an intention to damage a technical capability and impede the function of an entire system – for example, targeting industrial control systems or critical infrastructure.

StoneDrill

StoneDrill was discovered alongside Shamoon 2.0 in November 2016, as a new wave of wiper attacks targeted multiple victims in the Middle East. Despite similarities with the Shamoon malware from 2012, StoneDrill blurs the line between sabotage and espionage.

Like Flame, the StoneDrill malware has a wiper component and a backdoor. The wiper is not written to disk but instead is injected directly into the user's browser process memory [9]. This speaks to a general trend in the evolution and sophistication of malware – memory-resident malware leaves no trace of the file on disk, therefore legacy AV that is only file-based won't detect it. Most AV does now scan process memory, but the use of malware operating in memory still provides one less detection method.

The presence of the backdoor, along with command-and-control panels discovered by researchers [10], could suggest an espionage-oriented operation – though no public evidence has confirmed this.

It's worth noting that combining tools, such as a wiper and a backdoor, into one payload provides options for attackers to choose from depending on what is appropriate for the situation. Including a wiper and multiple other components could also prove to be beneficial because it provides more opportunities for a component to bypass the AV.

Interestingly, *FireEye* reported that StoneDrill was seen to be connected with APT33 [11]. Referred to as SHAPESHIFT, the wiper malware can wipe disks, erase volumes and delete files, but its use against targets remains unconfirmed. The appearance of SHAPESHIFT but restraint in its use could suggest signalling by the threat actor that it possesses destructive capabilities and a warning that they could be used in the future.

Shamoon 2.0

Returning after a four-year hiatus, Shamoon 2.0 first became known in November 2016 with two waves of attacks targeting Saudi organizations, and a third in January 2017. During the first stage, the attackers had stolen internal domain names and administrator credentials to access the victim network prior to the creation of the Shamoon 2.0 malware.

Whereas the original Shamoon only targeted filenames for exfiltration through a C&C, Shamoon 2.0 had initiated a separate operation prior to deploying the wiper, which stole credentials for future lateral movement. Shamoon 2.0 doesn't implement C&C communication.

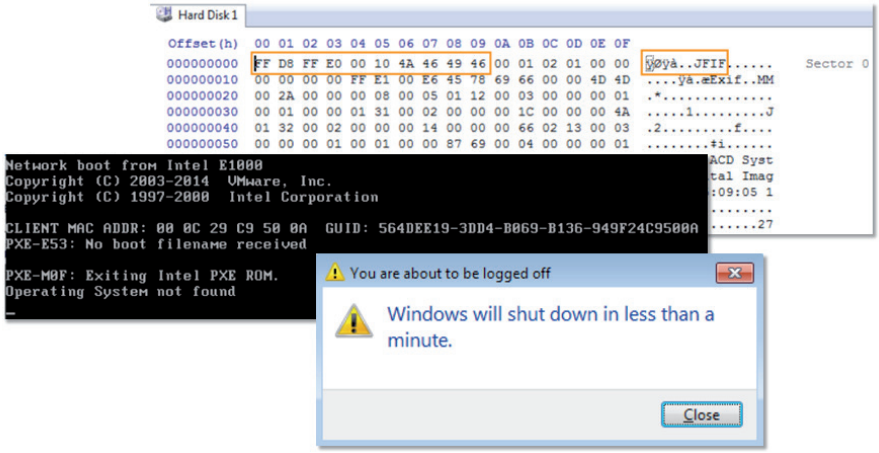

Figure 3: Shamoon 2.0

A less discussed aspect of Shamoon 2.0 was its fully functional ransomware module. At a specified time in the 32-bit version of the Shamoon dropper/worm, the malware drops a file that contains a public encryption key, though the file was unused in the Shamoon 2.0 attacks [12].

Shamoon 2.0 was built so that it could run as a wiper or as ransomware. The module is configured to wipe the disk with an image of the death of Alan Kurdi (Syrian child refugee). In the 64-bit Shamoon dropper, in its encryption mode, an RC4 key is generated, encrypted with the RSA public key and stored on the hard drive directly after the MBR.

The wiper function relies on the EldoS RawDisk driver to overwrite files on the system. It queries registry keys to obtain a list of partitions and certain files to overwrite, before rebooting. The EldoS RawDisk driver is used to circumvent the *Windows* API, allowing user-mode applications to interact with the file system in order to wipe it even if it is in use.

The wiper payload contains two configuration strings that designate which operations should be performed and how they should be performed. Examples include wiping/encrypting the Shamoon 2.0 components, user folders, partitions on hard disks, and the MFT on the system drive. The complexity of the wiper payload could indicate that the wiper was used quite heavily for many targets, where the attackers would want to easily configure options.

The implementation of selective, targeted wiping could be for the following reasons:

- The attackers were focused on destruction, and the best places to target would be the Documents or Downloads folders where important files are located.
- The attackers could have wanted more control over what happens on the machines.
- The attackers could have used filename results from Shamoon as information to curate future targets in the event of another attack. If particular filepaths were common, they would know where to target on the next run.

The presence of a C&C channel and transfer of filenames in Shamoon in 2012 remains unexplained but could suggest information gathering for future operations. The absence of any C&C communication in Shamoon 2.0 in 2016-2017 precludes the possibility of exfiltration and likely means the attack was focused purely on destruction.

DarkSeoul

In March 2013, three media organizations and six financial institutions in South Korea reported incidents that caused disruption and delay in their critical business. The South Korean government announced that over 30,000 hosts were affected.

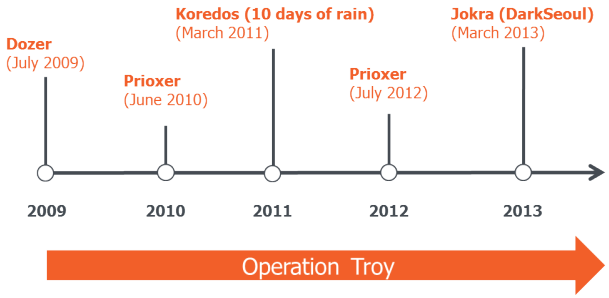

Figure 4: Extended DarkSeoul campaign timeline.

Three wipers were found in the investigation, all of which were designed to overwrite sections of the hard drive, including the MBR and VBR. The malware, which *Symantec* calls Trojan.Jokra, enumerates all drives and overwrites the MBR and the rest of the hard disk with a repeating string pattern – 'PRINCIPES' or 'HASTATI.'. It then forces the computer to restart, but it cannot boot because the MBR has been corrupted [13]. The malware doesn't possess a self-propagating capability. The dropper uses another (unknown) method to be delivered to the victim's host.

The first attacks on South Korea were in July 2009, with DDoS attacks against Korean and US government and financial websites. One wave of these attacks used the malware Dozer,

which contained a countdown to trigger an overwrite of files and the first megabyte of the hard drive on certain hard-coded dates. This would destroy the MBR and partition table.

In 2011, another DDoS attack took place alongside a similar wiper, Koredos [14], during '10 days of rain' [15]. Like the others, the wiper didn't contain any indication of espionage – no data exfiltration or backdoor functionality. However, a stealthy backdoor (Prioxer) was discovered in the process, a version of which also appeared in the DarkSeoul incident.

In their operations, the attackers used tactics to overwhelm (DDoS), to destroy (wiper), and even to steal (backdoor). While DarkSeoul itself was a sabotage operation, it was part of a larger espionage campaign named Operation Troy [16]. As part of Operation Troy, a military espionage campaign was conducted in parallel to the DarkSeoul attacks, in which variants of the Troy malware stole and exfiltrated sensitive military data. Similar to Shamoon, this illustrates how espionage and sabotage can be closely linked. The DarkSeoul attacks could even be classified as subversion – 'a deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order' [17].

NotPetya

When news of NotPetya first broke in June 2017, reporting suggested that it was a ransomware attack targeting businesses in Ukraine, Russia and Western Europe. Further investigation revealed that the attackers couldn't decrypt victims' disks after an email address linked to ransom collection was disabled, showing that NotPetya was a wiper disguised as ransomware.

NotPetya presents a unique case where both ransomware and a wiper were included in the attack, resulting in a blurred line between sabotage and diversion. The ransomware was used as a diversion, but the wiper itself was likely intended to sabotage businesses in Ukraine. The initial infiltration vector was via the compromised *MEDoc* software, allowing it to be distributed to a number of networks at the same time. This, combined with its worm-like capabilities which included a customized version of Mimikatz alongside the EternalBlue and EternalRomance exploits, makes it one of the first multi-propagation wipers.

Diversion

Attackers are using wipers in a new innovative way. Examples from the threat actor Lazarus show how a wiper is being deployed as a diversion, gaining the attention of IT and security teams, to ensure the attackers can manipulate their payment systems without scrutiny.

Hermes

In October 2017, reports emerged of a bank heist in Asia in which attackers targeted Far Eastern Bank International Bank in Taiwan and moved around $14.1 million from its accounts to overseas beneficiaries after compromising the bank's system connected to the SWIFT network. Along with known Lazarus tools, a piece of ransomware called Hermes was found in samples related to the intrusion [18].

Following the transfer of funds, the attackers executed the ransomware. This was compiled two days before the attack and consisted of a dropper that extracts the payload and spreads the ransomware to other computers via network shares. The dropper uses two sets of hard-coded credentials to spread to a hard-coded list of 5,357 internal IP addresses, which had likely been compiled from earlier reconnaissance.

The plain text ransom note is decrypted in memory but not written to disk due to a coding mistake. The ransomware writes and executes a batch script that deletes backups from the victim machine. At the end, the ransomware displays a message box with text – another mistake. These errors suggest the ransomware was compiled hastily, potentially still in testing and development, and ultimately the focus was on the impact of the delivery.

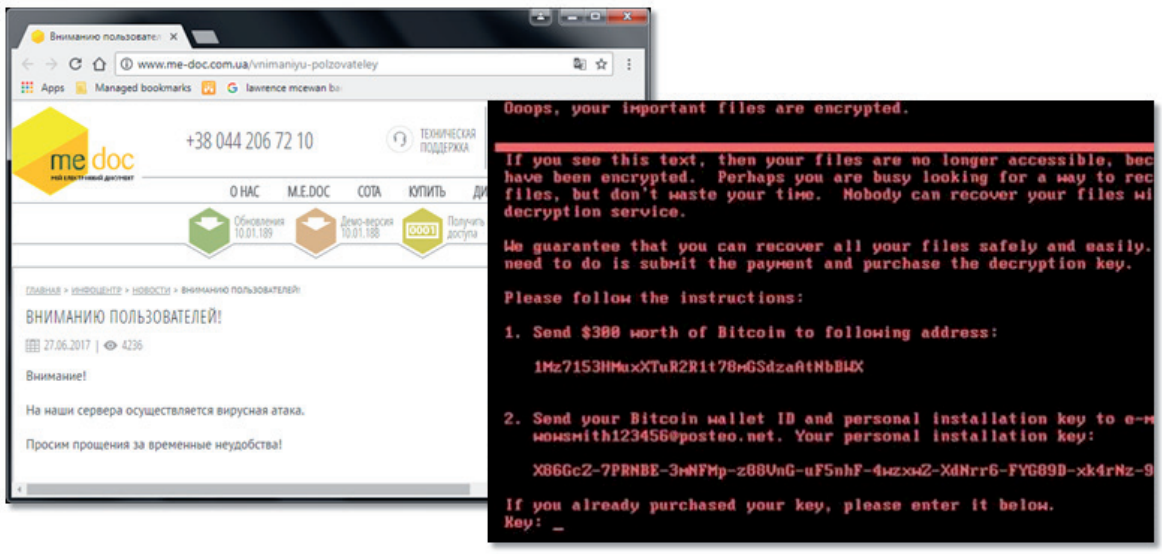

Figure 5: MEDoc software and NotPetya infected machine.

Lazarus continues to evolve its tactics to create new ways of disrupting victims and delaying their ability to respond. This was the first instance in which Lazarus employed a wiper in the form of a distraction, but subsequent cases show that this has become a part of the group's modus operandi.

MBR Killer

Lazarus appeared again in May 2018, this time in an attack on the Banco de Chile with a variant of KillDisk – MBR Killer.[4] As with other MBR wipers, the malware effectively makes the disk corrupt, but the files aren't overwritten; they still reside on the disk but the system can't identify the partitions.

The earliest public indication of a problem with Banco de Chile's computer systems came on 24 May, when some bank services became unavailable. The images posted by an IT professional on *Twitter* suggest that the bank's branch *Windows* IT systems are unable to boot – both images were posted on 24 May, the same day as the initial announcement of an issue by Banco de Chile [19, 20].

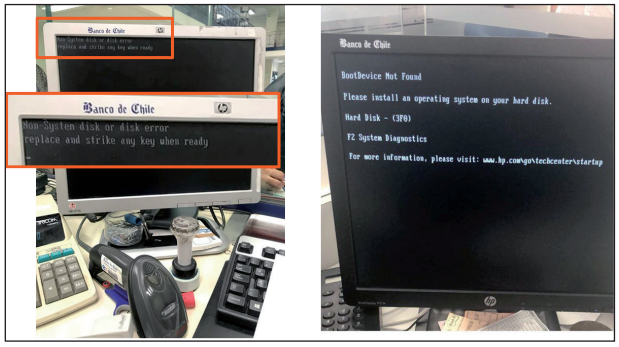

Figure 6: Banco de Chile infected branch computers.

MBR Killer is protected with *VMProtect*, a tool that has been used to obfuscate executables in previous bank heist activity, and even uses the same cracked version ('cracked by ximo'). However, samples similar to the MBR Killer sample investigated here have not been identified, suggesting this is a custom 'one-shot' tool, similar to Hermes in the Taiwan bank heist.

Lazarus has previously demonstrated an interest in compromising banks in Latin America. Banco de Chile also appears in the Lazarus watering hole whitelists from October 2016. While there is evidence that Lazarus gained access to bank networks many months before a well-timed heist attempt, it is not certain whether this watering hole (active 19 months before the Banco de Chile MBR Killer) was an initial compromise mechanism in this case.

It remains unknown how Lazarus deploys the destructive tools to potentially large numbers of machines simultaneously. No evidence of worm-like propagation has been shown in the analysis of these samples. If an attacker is inside a network with admin credentials to the domain, they could leverage legitimate processes already in place to deliver its malware. Lazarus could have gained access to configuration management servers and deployed the tools as 'updates'. One example could be to leverage an *SCCM* server (*Microsoft System Centre Configuration Manager*), a piece of software that facilitates managing a large number of computers on a network.[5]

Lazarus is also known for using tools that focus on wiping their own toolsets and logs (such as .tmp files), and code overlaps have shown variants of the same malware used in multiple attacks, likely due to their success. The emergence of secure wiping tools as part of the toolkit is a sophisticated tactic, hampering analysis, allowing the attackers to use their malware multiple times, without AV detection.

While Lazarus continues to use advanced tools to cover its activity and erase traces of its tools, the group has likely stockpiled many low-cost, low-sophistication wipers to use as distractions in what now has become standard practice in Lazarus bank heists.

CASE STUDY TAKEAWAYS

When looked at together (Figure 7), the case studies above demonstrate some trends across the uses of wipers.

WannaCry and NotPetya are key turning points for a couple of reasons. Despite there being several instances of sabotage over the last few years, none have had the sheer number of victims that WannaCry did. As shown in Figure 7, when there are only a few victims, the infiltration vector is usually a targeted intrusion. This is likely spear-phishing, though in many cases it remains unconfirmed. WannaCry and NotPetya demonstrated the mass abuse of an exploit – both resulting in a high volume of victims using a low-cost method and a publicly available tool.

When a new wiper tactic appeared – diversion – the attack was targeted, with only one victim. It's also worth noting that the same actor was behind the DarkSeoul attacks, Hermes and MBR Killer. Lazarus has shown a change in tactics using wipers where the modus operandi of destroying data and crippling systems is constant but uses different techniques – a traditional wiper or ransomware. Coupled with its strategic pivot from espionage and sabotage to diversion and financial gain, Lazarus' use of Hermes and MBR Killer marked a significant shift in how wipers are instrumented in cyber operations.

CONCLUSIONS

There are several conclusions and trends that emerge from the review of wipers in espionage, sabotage and diversion:

- A basic principle of wipers is separating their functionality from their intent/purpose. Wiper functionality is always to destroy data, but the classifications are where their intent lies. The use of wipers is a tactic, but espionage, sabotage and diversion are the strategies.

[4] A similar heist was attempted on Bancomext in Mexico in January 2018. Bancomext (Mexico's National Bank of Foreign Trade) suspended operations after a network failure and investigated an attempt to transfer funds to overseas bank accounts using an 'international payment platform'.

[5] *SCCM* can be used to deliver *Windows* updates, new software (remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory).

	Flame	Dark Seoul	Shamoon 2.0	WannaCry	NotPetya	Hermes	MBR Killer
Year	2010	2009-2013	2016-2017	2017	2017	2017	2018
Category	Espionage	Sabotage	Sabotage	Sabotage	Sabotage	Diversion	Diversion
Wiped Component	Log files and malware	MBR and files	Files	Files	MBR and files	Files and backups	MBR
Infection Vector	Targeted intrusion	Software update	Targeted intrusion	EternalBlue	Software update	Targeted intrusion	Targeted intrusion/ SCCM?
Propagation	Spooler and LNK exploits/software updates	Bash wiper script	Stolen creds	EternalBlue	EternalBlue/ Mimikatz	Domain admin privileges	Domain admin privileges (likely)
Victims	1	9	2	>200,000	100s	1	1

Figure 7: Wiper case study comparisons.

- Rather than being deployed in isolation, a wiper is often used in the context of a larger attack – whether complemented by other malware like a backdoor, or as a diversion for another part of the operation, or as a complement to a separate operation altogether. Some wipers are just components of larger payloads, which include other malware such as ransomware, backdoors, etc.
- Across classifications, wipers can cover tracks and complicate forensic investigation by erasing attacker activity logs. Depending on attacker motivation, this could be intentional artefact destruction to avoid attribution or a by-product of releasing the wiper to cause a system-wide impact.
- The wipers studied in this paper in general aren't that sophisticated, and they're all generally low-cost. More often than not, an operation using a wiper is about maximizing efficiency and impact for the least amount of investment. Wipers are a low-tech technique that yields a high impact.
- Wipers have become global in their reach and a staple in the arsenal of APT groups, marking a shift in the way states operate and conduct cyber operations. This is setting a precedent for nation states to use wipers in more and more contexts. We are going to continue to see an escalation in their deployment, perhaps for even more diverse purposes.
- Finally, like other intrusions, the geopolitical significance of many wiper attacks is that they show a manifestation of interstate conflict (Russia and Ukraine; North Korea and South Korea; the West and Iran; Iran and Saudi Arabia). The damage of infrastructure, the impact on economic processes, and the national security implications make the use of wipers a considerable threat.

REFERENCES

[1] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

[2] https://securelist.com/what-was-that-wiper-thing-48/34088/.

[3] https://www.talosintelligence.com/resources/58.

[4] https://blogs.cisco.com/security/talos/wiper-malware.

[5] http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf.

[6] https://securelist.com/full-analysis-of-flames-command-control-servers-27/34216/.

[7] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/analysis-flamer-cc-server-12-en.pdf.

[8] https://www.symantec.com/connect/blogs/flamer-urgent-suicide.

[9] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf.

[10] https://www.kaspersky.com/about/press-releases/2017_from-shamoon-to-stonedrill.

[11] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html.

[12] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf.

[13] https://www.symantec.com/connect/blogs/south-korean-banks-and-broadcasting-organizations-suffer-major-damage-cyberattack.

[14] https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise.

[15] https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf.

[16] https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf.

[17] http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf.

[18] http://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html.

[19] https://twitter.com/cafrati/status/999758905478733824.

[20] https://twitter.com/cafrati/status/999702915567751168.