Sandworm: A tale of disruption told anew

welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/

March 21, 2022

As the war rages, the APT group with a long résumé of disruptive cyberattacks enters the spotlight again

Rene Holt
21 Mar 2022 - 11:30AM

As the war rages, the APT group with a long résumé of disruptive cyberattacks enters the spotlight again

For cybersecurity pundits, it has become a doctrine that cyberdisruption, whether perpetrated directly or via proxy groups, can be expected to accompany military, political, and economic action as a way of softening up targets or of strategically applying pressure

via subterfuge. Thus, in a time of war in Ukraine, the spotlight has also naturally turned to cyberwarfare, both past and present.

Since at least 2014, companies in Ukraine or with network access to the region have suffered the likes of malware such as BlackEnergy, GreyEnergy, Industroyer, NotPetya, Exaramel, and, in 2022 alone, WhisperGate, HermeticWiper, IsaacWiper, and CaddyWiper. In all cases, except the last four, the cybersecurity community discovered enough code similarities, shared command and control infrastructure, malware execution chains and other hints to attribute all the malware samples to one overarching group – Sandworm.

Who is Sandworm?

The moniker Sandworm was chosen by researchers at iSIGHT Partners, a threat intelligence company, who discovered references to Frank Herbert's novel *Dune* in BlackEnergy malware binaries in 2014. At that time, ESET researchers were presenting their findings on several targeted BlackEnergy attacks in Ukraine and Poland at a Virus Bulletin conference, but also discovered the same, unmistakable references in the code: arrakis02, houseatreides94, BasharoftheSardaukars, SalusaSecundus2, and epsiloneridani0.

While some speculated that Sandworm was a group working from Russia, it wasn't until 2020 that the US Department of Justice (DoJ) concretely identified Sandworm as Military Unit 74455 of the Main Intelligence Directorate (GRU) – which was changed to the Main Directorate (GU) in 2010, although "GRU" seems to have stuck in Western parlance – of the General Staff of the Armed Forces of the Russian Federation, located at 22 Kirova Street, Khimki, Moscow in a building colloquially called "the Tower":

Figure 1. The Tower on 22 Kirova Street identified by the US DoJ as the location of GRU Unit 74455 (image source)

In his tome on Sandworm, Andy Greenberg reflected on his walk along the Moscow Canal below: “With my back to the canal, the Tower stood directly above me, blocked off by a high iron fence on a steep hill. I couldn’t make out a single human figure through its windows without using a pair of binoculars, which I wasn’t brave enough to try. It struck me that this was as close as I was likely ever going to get to the hackers I’d now been following for two years.”

The 2020 DoJ indictment that pulled the veil on Sandworm also named six officers of Unit 74455: Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin.

Figure 2. 'Wanted' poster for six members of GRU Unit 74455 (image source: FBI)

A 2018 indictment of the DoJ had named three additional officers of Unit 74455, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev.

As it is unlikely that these officers will ever be brought before a US court, it also appears unlikely for now to see what evidence the prosecutors might have to back the indictment. Publicly, this leaves the attribution of certain malicious campaigns to Sandworm based on these indictments alone on a more precarious footing. Yet where the two indictments incorporate information from public technical analyses of the malware attributed to Sandworm's subgroups, like BlackEnergy, TeleBots, and GreyEnergy, the attribution rests on much more solid ground.

Sandworm pummeling organizations far and wide

The sheer number of malicious campaigns and malware that have been linked to Sandworm over the years forms a litany of attacks that is difficult to summarize briefly. However, running through this list can give at least a broad perspective on the sophisticated capability demonstrated by this threat group.

BlackEnergy: From DDoS attacks to industrial control systems (2007–2015)

The first inklings of BlackEnergy's existence came in 2007 when Arbor Networks researchers identified a new botnet used by Russian hackers to conduct distributed denial-of-service attacks (DDoS) against Russian targets. BlackEnergy was sold by its original developer and used to strike Georgian websites with DDoS attacks when Russian troops hit the ground in Georgia in 2008.

In 2010, Dell SecureWorks released an analysis of a complete rewrite of the malware – BlackEnergy 2 – with new capabilities to hide as a rootkit, send spam, steal banking credentials, and destroy filesystems.

Then, in 2014, ESET discovered a variant of the malware, calling it BlackEnergy Lite due to its "lighter footprint." BlackEnergy Lite can execute arbitrary code and steal data from hard drives. Using a combination of both the regular and light versions, the BlackEnergy operators struck over a hundred targets in Poland and Ukraine, including governmental organizations.

The next time BlackEnergy reared its ugly head was in November 2015 when ESET observed it delivering a destructive KillDisk component against Ukrainian news media companies. KillDisk is a generic detection name for malware that overwrites documents with random data and makes the operating system unbootable.

A month later, in December, ESET detected another KillDisk variant at electricity distribution companies that appeared to contain functionality to sabotage specific industrial control systems. ESET also discovered SSHBearDoor, a backdoored SSH server used as an alternative to BlackEnergy for gaining initial access to systems. With this three-part toolset,

BlackEnergy caused a 4–6 hour power outage for around 230,000 people in the Ivano-Frankivsk region of Ukraine on December 23rd, 2015. This was the first time in history that a cyberattack was known to disrupt an electrical distribution system.

TeleBots targets financial institutions (2016)

ESET researchers discovered TeleBots, a successor of BlackEnergy, that was targeting financial institutions in Ukraine. TeleBots was named for its abuse of the Telegram Bot API to disguise the communication between the attackers and the compromised computers as HTTP(S) traffic to a legitimate server – api.telegram.org. The malware operators set up Telegram accounts from which they could issue commands to compromised devices. ESET researchers found a Telegram account belonging to one of the attackers.

As the final stage of these attacks, TeleBots deployed a destructive KillDisk variant that, instead of deleting files, replaced them with new files containing one of two strings: mrR0b07 or fS0cie7y – a callout to the Mr. Robot TV series.

ESET also discovered KillDisk fake ransomware variants capable of encrypting both Windows and Linux machines. After being encrypted, Linux machines became unbootable and displayed a ransom note for 222 Bitcoin, approximately US$250,000 at the time.

If the victims reached deep into their pockets to pay up, the attackers couldn't decrypt the files due to a deliberate flaw in the encryption scheme. However, ESET researchers did find a weakness in the encryption employed in the Linux version of the ransomware making recovery possible, albeit difficult.

Industroyer: Power outage in Kiev (2016)

On December 17th, 2016, almost a year after the first electrical power disruption in Ukraine, a second blackout occurred. The power was out for about an hour in part of the capital, Kiev. ESET researchers picked up new malware and named it Industroyer.

Industroyer is unique in its ability to speak several industrial communication protocols that are used worldwide in critical infrastructure systems for power supply, transportation control, water, and gas. Because these protocols were developed decades ago and were intended for use in offline systems, security was far from the foremost consideration in their design. Thus, once Industroyer achieved access to systems running these protocols, it became a simple matter to directly control the electricity substation switches and circuit breakers and turn off the power.

Figure 3. Protective relays for electrical substations – Industroyer spoke the language of this hardware

To clean up traces of itself after an attack, Industroyer's wiper module made systems unbootable and recovery harder by erasing system-crucial registry keys and overwriting files. At the time of this discovery, no connection was found between Industroyer and BlackEnergy.

RELATED READING: Industroyer2: Industroyer reloaded

US presidential campaign (2016)

In a year of intense political dueling between Donald Trump and Hillary Clinton for the US presidency, two GRU units came into view for disrupting Clinton's campaign. According to a DoJ indictment, Unit 26165 spearheaded a data leak campaign, hacking into the email accounts of members of Clinton's campaign and into the networks of the Democratic Congressional Campaign Committee and the Democratic National Committee.

Unit 74455 supported the leak of documents and emails stolen in these hacks. The attackers took on the fictitious personas DCLeaks, as well as Guccifer 2.0 in a copycat attempt of the original Guccifer who also leaked Clinton's emails back in 2013.

French presidential election (2017)

Similar to the hacks around the 2016 US presidential campaigns, Sandworm conducted seven spearphishing campaigns against the French presidential campaigns from April–May 2017, according to a DoJ indictment. More than 100 members of Emmanuel Macron's party *La République En Marche!*, along with other political parties and local government entities, were targeted.

The attackers set up a fake social media account to offer documents stolen from *En Marche!* and eventually leaked them.

TeleBots ransomware attacks preceding NotPetya (2017)

The infamous NotPetya (aka Diskcoder.C) attack was part of a series of ransomware attacks conducted in Ukraine by TeleBots. In 2017, ESET detected updated versions of TeleBots' tools along with two pieces of ransomware used in attacks against financial institutions in Ukraine.

In March, ESET detected the first of these TeleBots ransomware variants – Filecoder.NKH – which encrypted all files (except those located in the C:\Windows directory).

In May, a week after the WannaCryptor outbreak, ESET detected the second of these TeleBots ransomware samples – Filecoder.AESNI.C (aka XData). This ransomware is named from the fact that it checks whether a machine supports the Advanced Encryption Standard New Instructions (AES-NI) – a set of hardware instructions that speed up AES encryption and decryption.

ESET published a decryption tool for the Filecoder.AESNI ransomware.

NotPetya attack (2017)

In June 2017, a month after the infamous WannaCryptor attack, NotPetya struck organizations in Ukraine, rapidly spreading globally with worm-like capability via connected networks. Like WannaCryptor, NotPetya spread itself using an exploit known as EternalBlue, allegedly developed by the United States' National Security Agency and then stolen and dumped online by the Shadow Brokers hacking group. EternalBlue targets a critical flaw in an outdated version of Microsoft's Server Message Block (SMB) implementation, which is used mainly for file and printer sharing in corporate networks. NotPetya also spread using the EternalRomance exploit, another SMB exploit leaked by Shadow Brokers.

If successful, NotPetya encrypts either the entire drive or all files. At the time of the attack, IT admins rushed to shut down corporate computers before they could be sabotaged. For those that were struck, decryption was not possible even in the case of paying the US$300 ransom.

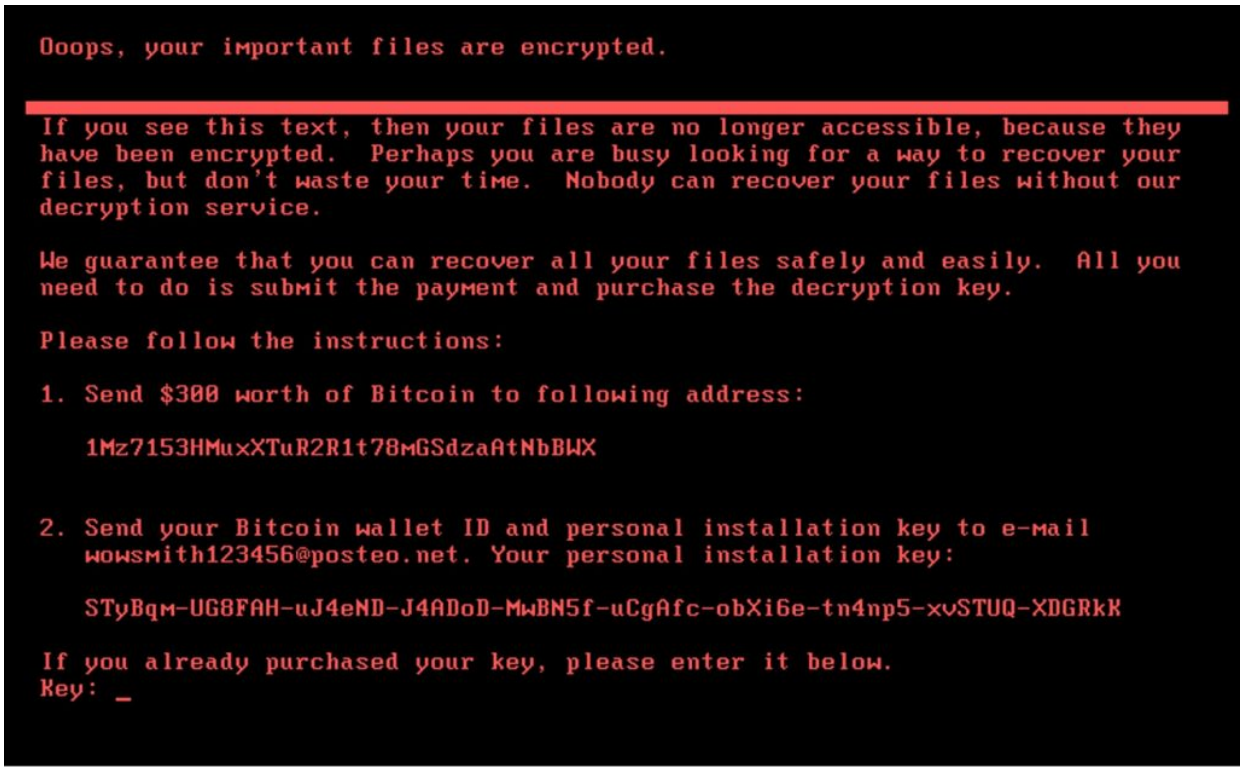

Figure 4. NotPetya ransom note

ESET researchers tracked the origin of this global malware epidemic to the supplier of the popular Ukrainian accounting software M.E.Doc. The NotPetya operators had compromised M.E.Doc's network and established access to an update server from which they sent a malicious update, unleashing NotPetya on the world. At the time, ESET attributed NotPetya to the TeleBots group.

In the current round of the MITRE Engenuity ATT&CK evaluations (2022), two threat actors are being put under the microscope: Wizard Spider and Sandworm. Both of these threat actors have deployed ransomware to disrupt the operations of victimized organizations. Wizard Spider used Ryuk ransomware for encryption, while Sandworm used NotPetya ransomware to destroy systems via encryption.

Olympic Destroyer impersonating Lazarus (2018)

While the opening ceremony of the PyeongChang 2018 Winter Olympic Games was a spectacular show for attendees, an unusually high number of seats were empty. Unbeknownst to the crowd, a cyberattack was taking place that shut down Wi-Fi hotspots and telecasts, grounded broadcasters' drones, took down the PyeongChang 2018 website, and broke the back-end servers of the Olympics' official app, preventing eager spectators from loading their tickets and attending the ceremony.

Two months earlier, the attackers had compromised the networks of two third-party IT companies contracted to support the IT operations of the PyeongChang Organizing Committee. On the fateful day of the ceremony – February 9th – it was an easy step for the attackers to pivot from these partner companies to PyeongChang Organizing Committee's

network and unleash Olympic Destroyer's wiper module, which deleted files and displayed BitLocker messages requesting a recovery key after a forced reboot, ultimately making them inoperable.

To better hide its origin, Olympic Destroyer's developers crafted some of the code to look like malware used by Lazarus, the APT group held responsible for the global WannaCryptor attack. A DoJ indictment attributed Olympic Destroyer to Sandworm, yet some researchers believe that Fancy Bear (aka Sofacy and APT28) was the more likely culprit.

Exaramel: Linking Industroyer to TeleBots (2018)

In April 2018, ESET discovered Exaramel, a new backdoor being used by the TeleBots group. When Industroyer knocked out the power in Ukraine in 2016, thoughts had immediately turned to the power outage triggered by BlackEnergy in 2015. However, there were no code similarities or other hints to link Industroyer to BlackEnergy or TeleBots. Exaramel was the missing piece of the puzzle.

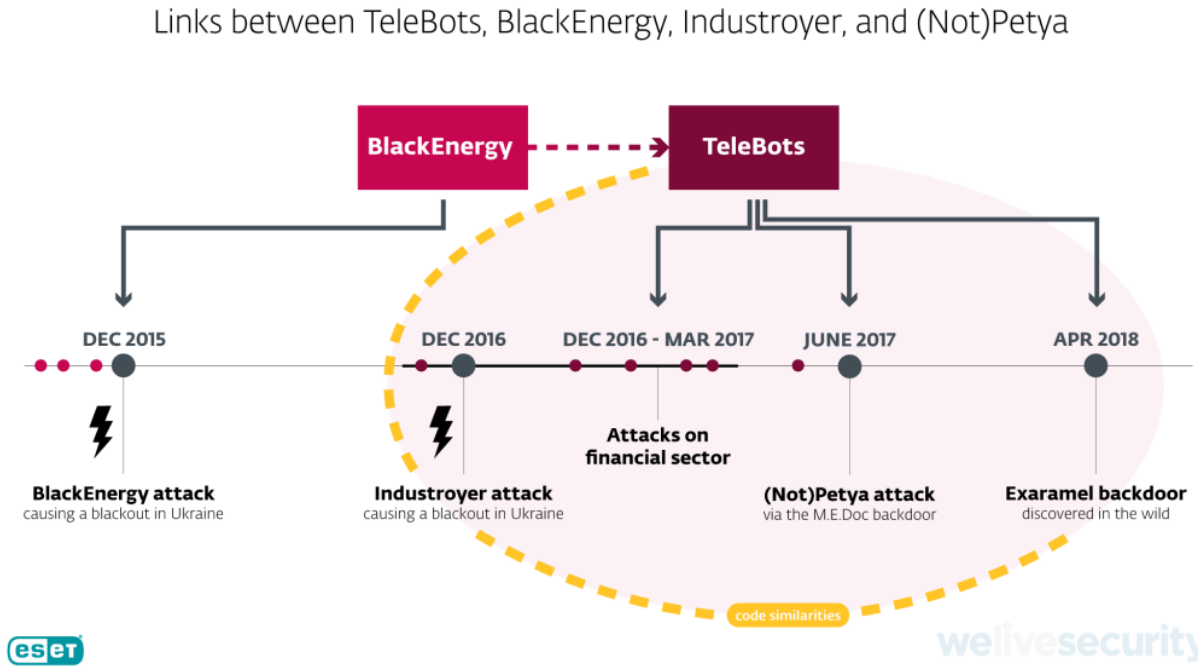

Figure 5. Links between TeleBots, BlackEnergy, Industroyer and (Not)Petya

The analysis of Exaramel revealed a number of similarities with Industroyer:

- both group their targets based on the security solution in use;
- both have very similar code implementation of several backdoor commands;
- both use a report file to store the output of executed shell commands and launched processes.

Additionally, Exaramel used the malicious domain um10eset[.]net, which was also used by a Linux version of TeleBots malware.

ESET also discovered a Linux variant of Exaramel equipped with the usual backdoor capabilities to establish persistence, communicate to its operators, execute shell commands, and download and upload files.

Unlike Industroyer, Exaramel doesn't directly target industrial control systems. ESET detected these Windows and Linux Exaramel backdoors at a Ukrainian organization that was not an industrial facility.

Similarly, in 2021, when France's national cybersecurity agency ANSSI released a report on a malicious campaign exploiting outdated versions of the Centreon IT monitoring tool, Exaramel reappeared, but again not at industrial facilities. Exaramel, in both its Windows and Linux variants, was discovered in the networks of web hosting providers in France.

GreyEnergy targets the energy sector (2015–2018)

Around the time of BlackEnergy's attack on Ukraine's electrical power grid in 2015, ESET started detecting malware that ESET researchers called GreyEnergy – another successor to BlackEnergy in parallel with TeleBots. While TeleBots focused on financial institutions, GreyEnergy mainly targeted energy companies in Ukraine, but also in Poland.

ESET was the first to document GreyEnergy's activities in 2018. The operators of this malware stayed out of the spotlight for three years, engaging in espionage and reconnaissance instead of destructive attacks like TeleBots' NotPetya and Industroyer.

GreyEnergy is similar to BlackEnergy but stealthier, wiping its malware components from victims' hard drives to avoid detection. In December 2016, ESET noticed that GreyEnergy deployed an early version of the NotPetya worm. After discovering that the malware authors had used the internal filename moonraker.dll for this worm – likely in reference to the James Bond film – ESET researchers eponymously named it Moonraker Petya.

Although ESET researchers did not find any GreyEnergy components that specifically target industrial control systems, the operators seemed to be targeting servers with high uptime and workstations used to manage industrial control systems.

Georgia (2019)

On October 28th, 2019, according to a DoJ indictment, Sandworm defaced around 15,000 websites hosted in Georgia, in many cases posting an image of Mikheil Saakashvili, a former Georgian president known for opposing Russian influence in Georgia, with the caption "I'll be back". The attack was orchestrated via a hack of Pro-Service, a Georgian web hosting provider.

The attack evoked memories of the BlackEnergy DDoS attacks on Georgian websites back in 2008.

Cyclops Blink (2022)

The day before Russia's invasion into Ukraine on February 24th, 2022, the US Cybersecurity and Infrastructure Security Agency (CISA) published an alert on Cyclops Blink, a newly discovered piece of Linux malware that enslaves WatchGuard Firebox devices to its botnet.

According to the technical analysis of the malware published by the UK's National Cyber Security Centre (NCSC), the malicious developers found a weakness that allowed the malware to pose as a legitimate firmware update of these devices. After a malicious update, to achieve persistence, a script automatically executes Cyclops Blink each time the compromised device restarts.

Cyclops Blink comes with a core component that poses as a kernel thread and several modules for gathering system information, downloading and uploading files, updating itself and persisting after reboot, and storing command and control server information.

While CISA has not yet revealed which hints led them to attributing Cyclops Blink to Sandworm, organizations are strongly advised to audit whether they have enabled the remote management interface to their Firebox devices, as this opens them immediately to these attacks without the patch.

Conclusion

Since February 24th, 2022, a host of malware targeting Ukrainian organizations, like HermeticWiper, HermeticWizard, HermeticRansom, IsaacWiper, and CaddyWiper has hit the headlines. Currently, the Hermetic malware family, IsaacWiper, and CaddyWiper remain unattributed, leaving one question hanging heavily in the air: Is Sandworm back to its mischief?

As cybersecurity vendors around the world continue to sift through their malware telemetry for clues, we may expect that more and more pieces of the puzzle will be put together. However, it may be that the disparate pieces will lead current theories increasingly astray. After all, skulduggery is part and parcel of the tactics employed by sophisticated threat groups.

One last word about keeping malware names straight. In the flurry of recent discoveries of malware in Ukraine, several of the same pieces of malware have been given different names. So, remember that HermeticWiper is the same as FoxBlade, and HermeticRansom is the same as Elections GoRansom, and PartyTicket.

21 Mar 2022 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion