An Overview of the Increasing Wiper Malware Threat

fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

April 28, 2022

In parallel with the war in Ukraine, cybersecurity researchers have witnessed a sudden increase in the number of wiper malware deployments. Although these haven't been officially attributed to Russian state-sponsored threat actors, their goals align with the Russian military's. It is widely theorized that these cyberattacks are intentionally being launched in concert with the invasion.

With wiper malware in the spotlight, we at FortiGuard Labs wanted to provide more information on this threat to help organizations understand it and implement better protections against them. In this blog, the following topics will be discussed:

- What is a wiper malware?
- The motivation for threat actors to use them
- Interesting properties that can influence the effectiveness of the malware
- Wiper techniques under the hood

- Protections provided by Fortinet

Definition

The wiper term in wiper malware comes from its most basic function, when the objective of the malware is to wipe (erase) the hard disk of the victim machine. More generically, wiper malware can be defined as malicious software that tries to destroy data. As we will see in the following sections, there are different ways to accomplish this.

History

Below is a short history of notable wiper malware (also shown in Figure 1):

- **Shamoon**, 2012: Used to attack Saudi Aramco and Qatar's RasGas oil companies.
- **Dark Seoul**, 2013: Attacked South Korean media and financial companies.
- **Shamoon**, 2016: Returned to again attack Saud Arabian organizations.
- **NotPetya**, 2017: Originally targeted Ukrainian organizations, but due to its self-propagation capability, it became the most devastating malware to date.
- **Olympic Destroyer**, 2018: Attack targeted against the Winter Olympics in South Korea.
- **Ordinypt/GermanWiper**, 2019: Targeted German organizations with phishing emails in German.
- **Dustman**, 2019: Iranian state-sponsored threat actors attacked Bapco, Bahrain's national oil company.
- **ZeroCleare**, 2020: Attacked energy companies in the Middle East.
- **WhisperKill**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **WhisperGate**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **HermeticWiper**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **IsaacWiper**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **CaddyWiper**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **DoupleZero**, 2022: Attacked Ukrainian organizations in parallel with the Ukraine-Russia war.
- **AcidRain**, 2022: Attacked Viasat's KA-SAT satellite service provider.

Figure 1: Wiper malware timeline

Motivation

In this section, we will look at the different motivations behind deploying a wiper malware. While its goals are straightforward, that does not mean that the motivation is always the same. We distinguish between the following four potential motivators: financial gain, destruction of evidence, sabotage, and cyberwar.

Financial Gain

In general, financial gain is the least significant motivator for wiper malware. This is understandable because it is hard to monetize destruction. However, one aspect we wanted to point out here is the fake ransomware variant that pretends to encrypt data and ask for a ransom, but without the capability to recover data. This could be called a ransomware scam because the ransomware concept is fraudulent. Threat actors employing such techniques are simply looking to make a quick buck without investing in developing an actual ransomware tool or in the administration work behind an actual ransomware operation. Of course, such an enterprise is short-lived because once it gets out that it is not possible to recover data, nobody will pay the ransom.

A good example is the **Ordinypt** or **GermanWiper,** which was active in 2017. As ransomware does, it altered files and added a random 5-character extension to them. It also destroyed recovery options, such as the Windows shadow copy. And it changed the desktop background to display a ransom note with a Bitcoin address where the ransom payment was expected to be sent. However, it did not really encrypt files. Instead, it filled them with zero bytes and truncated them. With this approach, there was no way to recover any affected files.

Destruction of Evidence

This is a hard-to-prove motivator, but sometimes when there is no other reason to deploy a wiper in an attack, it may be concluded that the real reason was something else, such as espionage. The wiper is only deployed after the true goal of the attack is achieved. Instead of meticulously erasing their tracks and all evidence of their attack, the attackers simply deploy a wiper malware in the organization. This not only erases the evidence, but the scale of the destruction causes the defenders to focus on the recovery of data and operations and not on investigating the intrusion.

Sabotage

Sabotage is the most obvious reason to deploy a wiper. Just as the Stuxnet malware was used to destroy centrifuges to slow down Iran's efforts to develop nuclear weapons, wiper malware could be used to destroy data, sabotage development, cause financial loss, or just cause chaos.

One example in this category is the **Shamoon** malware, used to attack Saudi Aramco and other oil companies. The attack destroyed 30,000 workstations at Saudi Aramco. At such a scale, even replacing these computers becomes a logistical nightmare. The attack was also scheduled for a time when a holiday had just started to maximize its impact by counting on the limited staff available to respond to the attack.

Cyberwar

A few months ago, it would not have been as straightforward to include this motivation in the list. But at the time of this post, seven different wiper malware attacks (WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AcidRain) have been discovered targeting Ukrainian infrastructure or Ukrainian companies—all clearly in line with Russia's interest in the Ukraine-Russia war. Generally, wiper operations in this category attack targets whose destruction is in the interest of the opposing military. For example, the motivation behind such an attack might be to cripple critical infrastructure. This could be done to either cause chaos and increase mental stress on the enemy or to cause destruction at a tactical target. Wiper attacks can also have a devastating effect against OT and critical infrastructure targets, which has its value in a war.

An interesting and recent example is the suspicion that the **AcidRain** wiper was used in an attack against the Viasat KA-SAT satellite broadband service provider. The attacker gained access to the management infrastructure of the provider to deploy AcidRain on KA-SAT modems used in Ukraine. The attack also rendered 5,800 wind turbines inaccessible in Germany.

Interesting Properties

Although the general objective of wiper malware is quite simple, some have interesting properties worth discussing.

Fake Ransomware

As discussed, many wiper malware samples pretend to be ransomware. This means they leverage many of the typical Tactics, Techniques, and Procedures (TTP) that actual ransomware uses, but they do this without the possibility of recovering the files. In theory, standard ransomware can also be used as a wiper if the decryption key is never provided to the victim. In that case, the encrypted files are practically lost. However, after detailed analysis, it is apparent in many cases that the ransomware functionality is just a ruse, and in reality, the malware is a wiper. There could be a couple of reasons to do this:

- As seen previously with Ordinypt, a sample can follow the ransomware business model without the intention to recover files.
- It can be used to mislead the incident response team and, with that, slow down countermeasures.

- Hide the motivation behind an attack. Ransomware would suggest cybercrime, which could be a way to hide that the real motivation is sabotage or cyberwar.

An excellent example of the latter is the infamous **NotPetya** malware from 2017. It was the most devastating malware so far. It started with a supply chain attack against Ukrainian companies through updates from a small Ukrainian accounting software company. However, it did not stop there. Since NotPetya was a worm, it also exploited vulnerabilities in other software to propagate. This was so efficient that it quickly became a global problem, crippling networks without discrimination. It went to great lengths to imitate ransomware, such as encrypting files, providing a Bitcoin address for payment, and delivering a ransom note. However, in reality, it was a wiper that just destroyed data. It was attributed to the Sandworm actors, who are associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, often referred to as GRU.

Self-Propagation

As with NotPetya, we can see that a significant property of wipers is whether or not they are self-propagating. If it is a worm, such as NotPetya, it will self-propagate to other machines once it is let loose. It is not necessarily possible to control them any longer in such a case.

There are a couple of ways malware can self-propagate:

- By exploiting vulnerabilities in-network services.
- Gathering credentials on infected machines and using them to connect to other machines in the network.
- Using legitimate ways to move from one device to another, such as update processes.

This does not mean, of course, that non-self-propagating malware cannot be devastating. If the domain controller is compromised in a network, it can be used to deploy the wiper on all machines in the organization. The main difference is that self-propagating malware cannot be controlled once it has been unleashed.

Wiping Techniques

Now let's roll up our sleeves and get our hands dirty by looking under the hood of wiper malware to understand the techniques they use to destroy the victim's data.

Overwriting Files

The most trivial approach for wipers is to simply enumerate the filesystem and overwrite the selected files with data. We discussed earlier that Ordinypt used this approach, overwriting files with zero (0x00) bytes.

Another good example is the **WhisperGate** wiper deployed against Ukrainian organizations earlier this year. It had various stages and components, but the second stage (stage2.exe) downloaded the file corrupter component from a hardcoded Discord channel. This component goes through specific folders looking for files with file extensions hardcoded in the malware. These files are different data files. The malware replaces the content of the files with 1 MB of 0xCC bytes and adds a 4-character long random extension. It is worth noting that WhisperGate also pretended to be ransomware, even though it corrupts files beyond repair.

Encrypting Files

As mentioned earlier, encrypting a file and destroying the key is essentially equivalent to destroying the file. Of course, a brute-force attempt could be made to recover the file, but if proper encryption algorithms are used, this approach is quite hopeless. However, encryption rather than simply overwriting is very resource-intensive and slows down the malware. The only use case for implementing encryption in a wiper is when the authors want to keep up the appearance of being ransomware for as long as possible. This was the case with NotPetya, which did encrypt files properly.

Overwriting MBR

Many wipers also make sure to overwrite the Master Boot Record (MBR) of the disk. This part of a disk tells the computer how to boot the operating system. If the MBR is destroyed, the computer won't start. However, this does not mean that the data on the hard disk has been destroyed. If only the MBR is corrupted, the data can still be recovered. By itself, it can only be used to cause chaos and confusion, but no actual data loss. That is why it is usually used together with other techniques.

For instance, the **ZeroCleare** malware used against energy companies in the Middle East in 2019 also used this technique. It used the third-party driver management tool EldoS RawDisk (more on that later) to directly access hard drives bypassing the protection mechanisms of the operating system (OS). Instead of overwriting files on the OS level, ZeroCleare overwrites the disks directly with 0x55 bytes. This, of course, starts with the MBR and continues with all partitions. A very clever technique we should mention when talking about ZeroCleare is that it bypassed the Windows Driver Signature Enforcement(DSG), which protects Windows from loading unsigned drivers (RawDisk driver). To do that, it first loaded a publicly available known vulnerable signed driver of VirtualBox. It then exploited the vulnerability in this legitimate driver to load RawDisk's unsigned driver. Once that happened, it had direct access to the disks in the machine.

Overwriting MFT

MFT stands for Master File Table, and it exists on every NTFS filesystem. This is basically a catalog of all the files that exist on the filesystem, their metadata, and either the file content or the location where the file content is stored. If the MFT is corrupted, the operating system won't be able to find the files. This is a very easy and fast way for wiper malware to make files disappear. The one drawback is similar to corrupting the MBR: the file content is not necessarily destroyed. While the few files stored directly in the MFT would be erased, most of the files are stored somewhere else on the disk, and the MFT only provides their location to the OS. Without the MFT, the OS won't be able to find the content, but the content is still there on the disk.

A fascinating example is **NotPetya** again. It overwrote the MBR of the target machine with a custom boot loader and stored a custom low-level code that this boot loader called. This code encrypted the MFT when the first restart happened after the infection. Once the MFT was encrypted, it forced the machine to restart. After that second restart, the device would no longer boot but only display the ransom note (Figure 2).

Figure 2: NotPetya ransom note

Using IOCTL

IOCTL is the device input and output control interface in Windows. The DeviceIoControl() function is a general-purpose interface used to send control codes to devices. The control codes are essentially operations to be executed by the device driver. Malware uses this interface to collect information about the disks targeted for the actual wiping.

In the case of **HermeticWiper**, IOCTLs were used for the following purposes:

- Drive fragmentation (as opposed to defragmentation): spreading files around the drive makes a recovery more difficult. To achieve this, the FSCTL_GET_RETRIEVAL_POINTERS and FSCTL_GET_MOVE_FILES IOCTL codes are used.
- Parsing the drive's contents to identify the parts to be destroyed: To do this, the IOCTL_DISK_GET_DRIVE_LAYOUT_EX and IOCTL_DISK_GET_DRIVE_GEOMETRY_EX codes are used.
- Collecting occupied clusters to stage them for erasing: This is a performance improvement to ignore clusters not in use. For this, the FSCTL_GET_VOLUME_BITMAP and FSCTL_GET_VOLUME_BITMAP IOCTLs codes are used.
- And finally, the FSCTL_GET_NTFS_FILE_RECORD code is used to load a record from an NTFS filesystem.

Once HermeticWiper collects all the data it wants to erase to maximize the impact of the wiping, it uses the EaseUS Partition Master driver to overwrite the selected parts of the disk with random data.

Third-party tooling

It was previously mentioned that malware sometimes uses third-party tools to overwrite data. They usually use the Windows driver of off-the-shelf products to bypass the protection mechanisms of Windows and manipulate the disks directly. The primary reason for using third-party drivers is probably that poorly implemented drivers can easily crash the whole system, which would lead to investigation and detection. Attackers likely don't want to invest time into writing their own drivers. Another reason might be that only signed drivers are allowed to be loaded on modern Windows systems, so if they wrote their own driver, they would need to bypass this security mechanism. This is, of course, not impossible, as we saw with ZeroCleare, which first loads a signed but vulnerable driver and then exploits that vulnerability to load the unsigned driver.

The two most widely-used examples of third-party tools used are:

- EldoS RawDisk, used by the Shamoon and ZeroCleare wipers and the Lazarus Group in their infamous Sony Hack.
- EaseUS Partition Master used by HermeticWiper

All of the Above

As shown in the examples above, most wipers are not using just one technique but a combination. Wipers employ varying complexity in trying to reach their goals. The more complex the malware is, the more techniques it needs to use. And, of course, the more techniques are used, the lower the probability that the data can be recovered.

Fortinet Telemetry

Figure 3 shows Fortinet Anti-Virus (AV) detection numbers since January 2022 of various wiper malware signatures. We can see that there was a significant increase. It is also interesting to see that there is still a lot of NotPetya detection, which can be explained by the fact that it is a worm so as long as there are vulnerable machines out there NotPetya will keep self-propagating. We can also see how the war specific new wipers appeared in March and increased the numbers significantly.

Figure 3: AV detection for wiper samples since January

Recommendations

There are several best practices organizations are urged to implement to minimize the impact of wiper malware:

Backup: The most helpful countermeasure for ransomware and wiper malware is to have backups available. Malware often actively searches for backups on the machine (such as Windows Shadow Copy) or on the network to destroy. Therefore, backups must be stored off-site and off-line to survive sophisticated attacks. And when we talk about backups, it is important to mention that the existence of backups is essential, but a detailed recovery process also exists. And that the IT team regularly exercises recovery from backup to minimize downtime.

Segmentation: Proper network segmentation can be useful on multiple levels. For example, it can limit the impact of an attack to one segment of the network. In addition, firewalls used in combination with anti-virus and intrusion prevention systems, such as FortiGate, FortiGuard IPS, and FortiGuard Content Security, can detect the propagation of malware on the network, communications to known command and control servers, and malicious files as they are moved through the network.

Disaster recovery plan: Once a wiper is deployed in the network, the question is how well is the organization prepared for such a situation. What processes have been defined for business continuity without IT? How will restoration from backups be done and how will the organization communicate the incident to customers and the media? These are all questions that should be settled before an attack. All this and more should be defined in a disaster recovery plan, which will be invaluable under the extreme stress of an active compromise.

Incident Response: The speed and the quality of incident response are crucial, and the outcome of the attack can highly depend on it. In a scenario where a compromise is detected before wiper malware is deployed, the manner in which the incident response team handles and responds to the compromise could mean the difference between successfully averting data loss and complete data destruction. The FortiGuard Incident Response & Readiness Services is a trusted partner of many organizations for just this purpose.

Fortinet Protection

Fortinet products detect all malware discussed in this blog.

Fortinet Anti-Virus Signatures

HermeticWiper:
W32/KillDisk.NCV!tr
W32/Agent.OJC!worm

IsaacWiper:
W32/KillMBR.NHQ!tr

CaddyWiper:
W32/CaddyWiper.NCX!tr

WhisperKill:
W32/KillFiles.NKU!tr.ransom

WhisperGate:
W32/KillMBR.NGI!tr
MSIL/Agent.FP!tr.dldr
MSIL/Agent.QWILJV!tr
W32/KillFiles.NKU!tr.ransom
MSIL/VVH!tr
MSIL/Agent.VVH!tr

Shamoon:
W32/DISTTRACK.C!tr
W32/Generic.BQYIIWO!tr
W64/DistTrack.A!tr
Malware_Generic.P0
DistTrack.Botnet

Ordinypt:
W32/Ordinypt.5873!tr.ransom

Olympic Destroyer:
W32/OlympicDestroyer.A!tr

NotPetya:
W32/Petya.EOB!tr
W32/Petya.A!tr.ransom
W64/Petya.BG!tr

Dustman:
W32/Agent.F0FC!tr
W64/Dustman.KH!tr
W32/Distrack!tr

ZeroCleare:
W32/Agent.XACVYS!tr
W32/Distrack!tr

DoubleZero:
MSIL/DZeroWiper.CK!tr

AcidRain:
ELF/AcidRain.A!tr

IOCs (SHA-256 hashes of samples)

Shamoon:

128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd
394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b
448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237
47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34
61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842
772ceedbc2cacf7b16ae967de310350e42aa47e5cef19f4423220d41501d86a5
c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6
5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a

Ordinypt

085256b114079911b64f5826165f85a28a2a4ddc2ce0d935fa8545651ce5ab09

Olympic Destroyer:

edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9
19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf3476e0cc30ebea
ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da9456e2d5885c7f
f188abc33d351c2254d794b525c5a8b79ea78acd3050cd8d27d3ecfc568c2936
ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2e91790f052c85
D934CB8D0EADB93F8A57A9B8853C5DB218D5DB78C16A35F374E413884D915016
EDB1FF2521FB4BF748111F92786D260D40407A2E8463DCD24BB09F908EE13EB9
3E27B6B287F0B9F7E85BFE18901D961110AE969D58B44AF15B1D75BE749022C2
28858CC6E05225F7D156D1C6A21ED11188777FA0A752CB7B56038D79A88627CC

NotPetya:

be2fb06b0a61f72d901ea3d650912bb12ef94896528cca6f8f9466e49c1d0721
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998
02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f

Dustman:

18c92f23b646eb85d67a890296000212091f930b1fe9e92033f123be3581a90f
f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7
2fc39463b6db44873c9c07724ac28b63cdd72f5863a4a7064883e3afdd141f8d

ZeroCleare:

becb74a8a71a324c78625aa589e77631633d0f15af1473dfe34eca06e7ec6b86
2fc39463b6db44873c9c07724ac28b63cdd72f5863a4a7064883e3afdd141f8d
05aae309d7a8c562b3cf364a906b3fcb764c122855c7260697d96f83fc8ccee8

HermeticWiper:
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

IsaacWiper:
13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033

CaddyWiper:
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
b66b179eac03afafdc69f62c207819eceecfbf994c9efa464fda0d2ba44fe2d7

WhisperGate:
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

WhisperKill:
34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907
191ca4833351e2e82cb080a42c4848cfbc4b1f3e97250f2700eff4e97cf72019
24e9b86b92918c3731fa6126c70532c79507c8041b8e6bf1e1c007aa8a9ac025
6aa4081d4028116bb50315774f0d5dfd45dfb9b9f61f172cfa53bfc65eddf229

DoubleZero:
3b2e708eaa4744c76a633391cf2c983f4a098b46436525619e5ea44e105355fe
8dd8b9bd94de1e72f0c400c5f32dcefc114cc0a5bf14b74ba6edc19fd4aeb2a5
30b3cbe8817ed75d8221059e4be35d5624bd6b5dc921d4991a7adc4c3eb5de4a
d897f07ae6f42de8f35e2b05f5ef5733d7ec599d5e786d3225e66ca605a48f53

AcidRain
9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a

ATT&CK TTPs

ID	Name
T1485	Data Destruction
T1486	Data Encrypted for Impact

T1561	Disk Wipe
T1561.001	Disk Wipe: Disk Content Wipe
T1561.002	Disk Wipe: Disk Structure Wipe
T1495	Firmware Corruption
T1529	System Shutdown/Reboot
T1053.005	Scheduled Task/Job: Scheduled Task
T1569.002	System Services: Service Execution
T1542.001	Pre-OS Boot: System Firmware
T1542.002	Pre-OS Boot: Component Firmware
T1542.003	Pre-OS Boot: Bootkit
T1006	Direct Volume Access
T1562.001	Impair Defenses: Disable or Modify Tools
T1070.004	Indicator Removal on Host: File Deletion
T1083	File and Directory Discovery

Further Reading

Shamoon - https://www.fortinet.com/blog/threat-research/research-furtive-malware-rises-again

Olympic Destroyer - https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

Dustman - https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/

NotPetya - https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

NotPetya - https://www.fortinet.com/blog/threat-research/key-differences-between-petya-and-notpetya

ZeroCleare - https://www.ibm.com/downloads/cas/OAJ4VZNJ

CaddyWiper - https://www.fortiguard.com/encyclopedia/virus/10082978

HermeticWiper - https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/

WhisperGate - https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

AcidRain - https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

DoubleZero - https://cert.gov.ua/article/38088

WhisperKill - https://cert.gov.ua/article/18101

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.