Behavior monitoring combined with machine learning spoils a massive Dofoil coin mining campaign | Microsoft Security Blog

By Microsoft Defender Security Research Team

Published: 2018-03-07 · Archived: 2026-04-05 17:39:26 UTC

Update: Further analysis of this campaign points to a poisoned update for a peer-to-peer (P2P) application. For more information, read **Poisoned peer-to-peer app kicked off Dofoil coin miner outbreak**. To detect and respond to Dofoil in corporate networks, read **Hunting down Dofoil with Windows Defender ATP**.

Just before noon on March 6 (PST), Windows Defender Antivirus blocked more than 80,000 instances of several sophisticated trojans that exhibited advanced cross-process injection techniques, persistence mechanisms, and evasion methods. Behavior-based signals coupled with cloud-powered machine learning models uncovered this new wave of infection attempts. The trojans, which are new variants of Dofoil (also known as Smoke Loader), carry a coin miner payload. Within the next 12 hours, more than 400,000 instances were recorded, 73% of which were in Russia. Turkey accounted for 18% and Ukraine 4% of the global encounters.

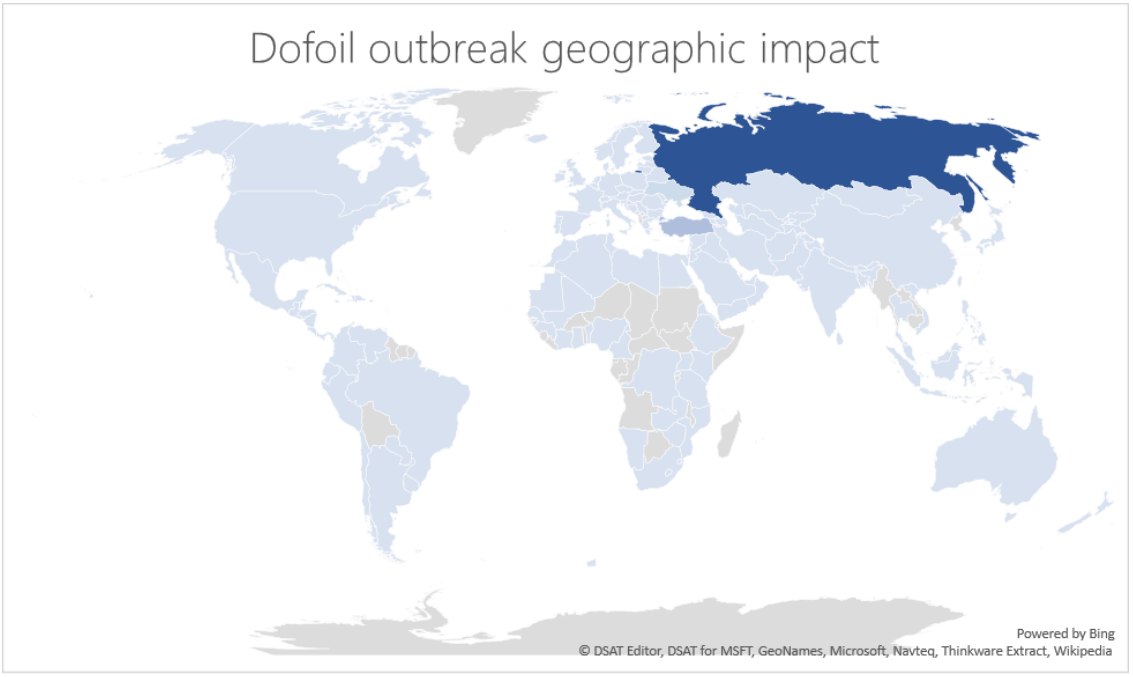


Figure 1: Geographic distribution of the Dofoil attack components

Windows Defender AV initially flagged the attack's unusual persistence mechanism through behavior monitoring, which immediately sent this behavior-based signal to our cloud protection service.

1. Within milliseconds, multiple metadata-based machine learning models in the cloud started blocking these threats at first sight.

2. Seconds later, our sample-based and detonation-based machine learning models also verified the malicious classification. Within minutes, detonation-based models chimed in and added additional confirmation.
3. Within minutes, an anomaly detection alert notified us about a new potential outbreak.
4. After analysis, our response team updated the classification name of this new surge of threats to the proper malware families. People affected by these infection attempts early in the campaign would have seen blocks under machine learning names like Fuery, Fuerboos, Cloxer, or Azden. Later blocks show as the proper family names, Dofoil or Coinminer.

Windows 10, Windows 8.1, and Windows 7 users running Windows Defender AV or Microsoft Security Essentials are all protected from this latest outbreak.

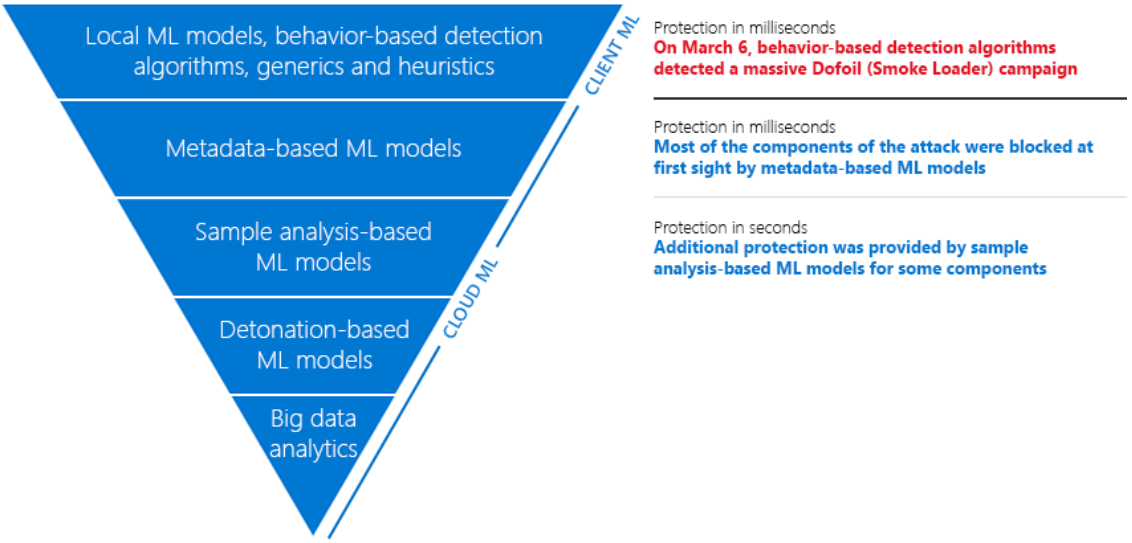
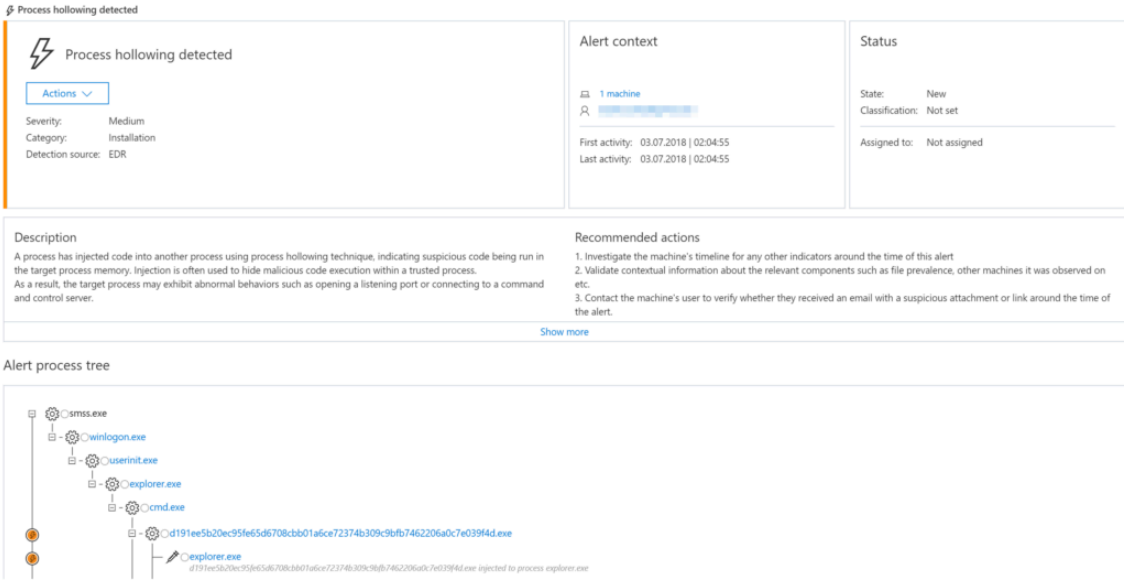


Figure 2. Layered machine learning defenses in Windows Defender AV

Artificial intelligence and behavior-based detection in Windows Defender AV has become one of the mainstays of our defense system. The AI-based pre-emptive protection provided against this attack is similar to how layered machine learning defenses stopped an Emotet outbreak last month.

Code injection and coin mining

Dofoil is the latest malware family to incorporate coin miners in attacks. Because the value of Bitcoin and other cryptocurrencies continues to grow, malware operators see the opportunity to include coin mining components in their attacks. For example, exploit kits are now delivering coin miners instead of ransomware. Scammers are adding coin mining scripts in tech support scam websites. And certain banking trojan families added coin mining behavior.



The Dofoil campaign we detected on March 6 started with a trojan that performs process hollowing on *explorer.exe*. Process hollowing is a code injection technique that involves spawning a new instance of legitimate process (in this case *c:\windows\syswow64\explorer.exe*) and then replacing the legitimate code with malware.

Figure 3. Windows Defender ATP detection for process hollowing (SHA-256: d191ee5b20ec95fe65d6708cbb01a6ce72374b309c9bfb7462206a0c7e039f4d, detected by Windows Defender AV as TrojanDownloader:Win32/Dofoil.AB)

The hollowed explorer.exe process then spins up a second malicious instance, which drops and runs a coin mining malware masquerading as a legitimate Windows binary, wuauclt.exe.

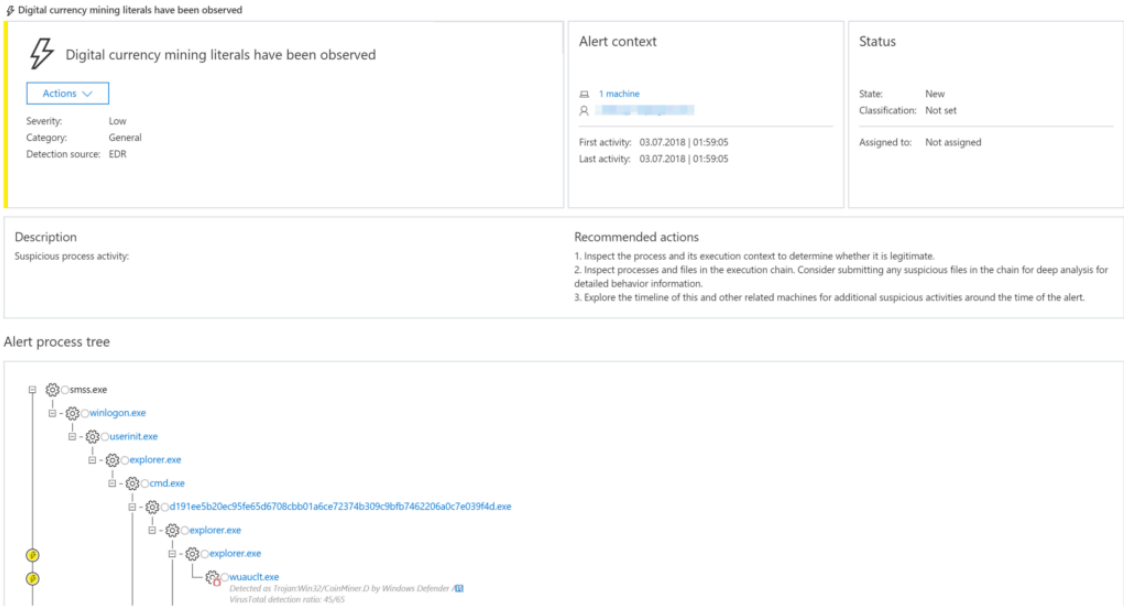


Figure 4. Windows Defender ATP detection for coin mining malware (SHA-256: 2b83c69cf32c5f8f43ec2895ec9ac730bf73e1b2f37e44a3cf8ce814fb51f120, detected by Windows Defender AV as Trojan:Win32/CoinMiner.D)

Even though it uses the name of a legitimate Windows binary, it's running from the wrong location. The command line is anomalous compared to the legitimate binary. Additionally, the network traffic from this binary is suspicious.

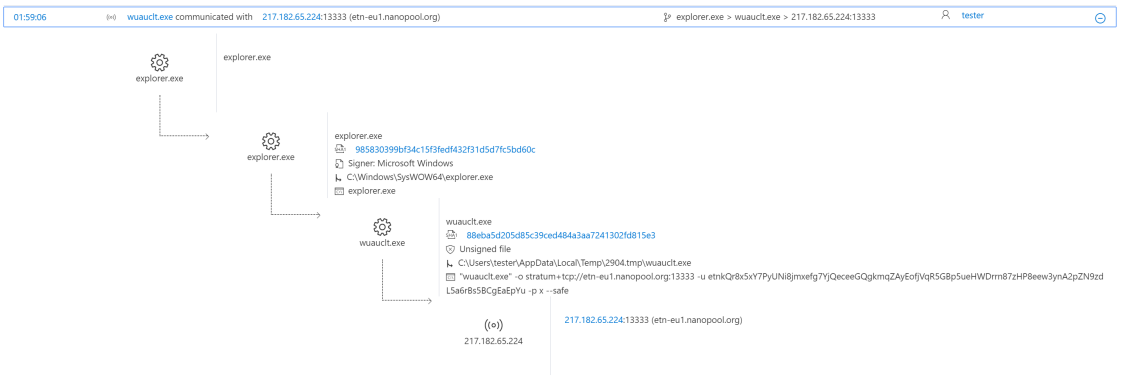


Figure 5. Windows Defender ATP alert process tree showing anomalous IP communications

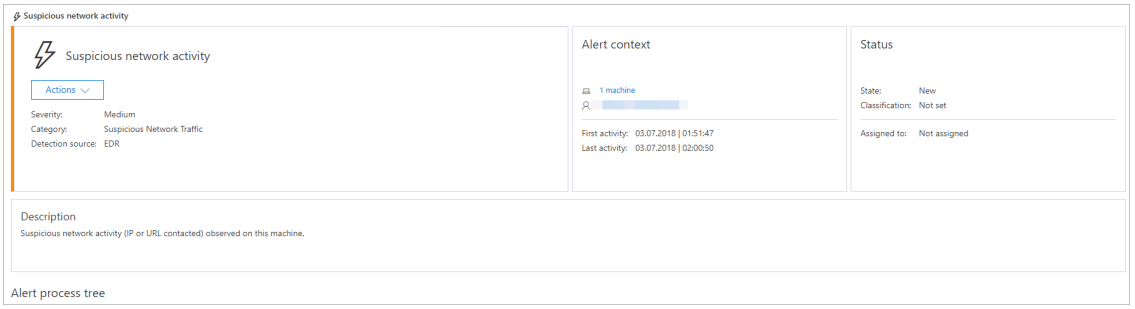


Figure 6. Windows Defender ATP showing suspicious network activity

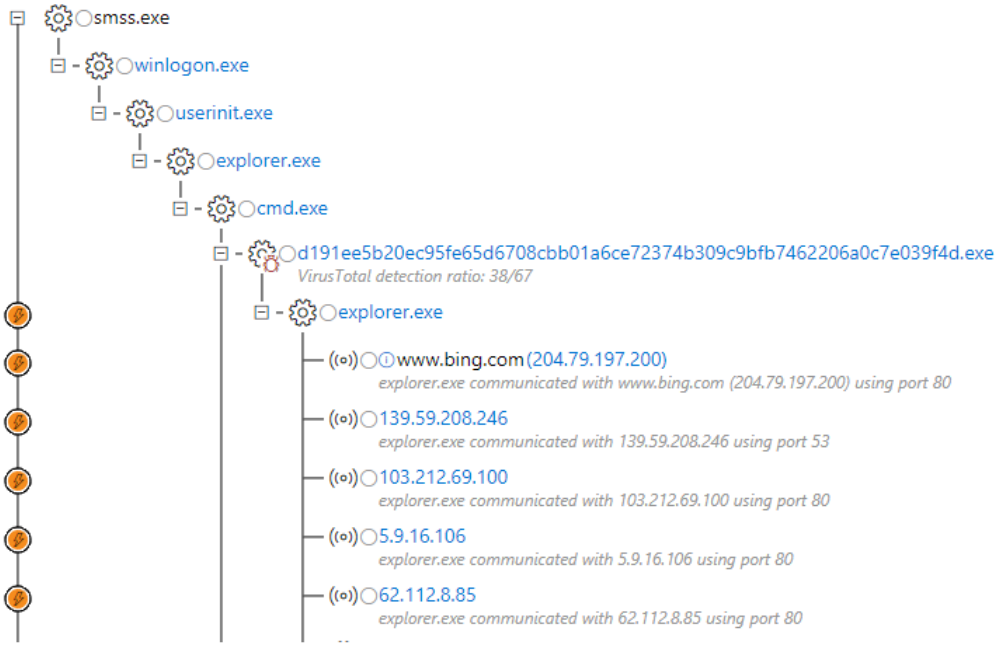


Figure 7. Windows Defender ATP alert process tree showing hollowed explorer.exe process making suspicious connections

Dofoil uses a customized mining application. Based on its code, the coin miner supports NiceHash, which means it can mine different cryptocurrencies. The samples we analyzed mined Electroneum coins.

Persistence

For coin miner malware, persistence is key. These types of malware employ various techniques to stay undetected for long periods of time in order to mine coins using stolen computer resources.

To stay hidden, Dofoil modifies the registry. The hollowed *explorer.exe* process creates a copy of the original malware in the Roaming AppData folder and renames it to *ditereah.exe*. It then creates a registry key or modifies an existing one to point to the newly created malware copy. In the sample we analyzed, the malware modified the OneDrive Run key.

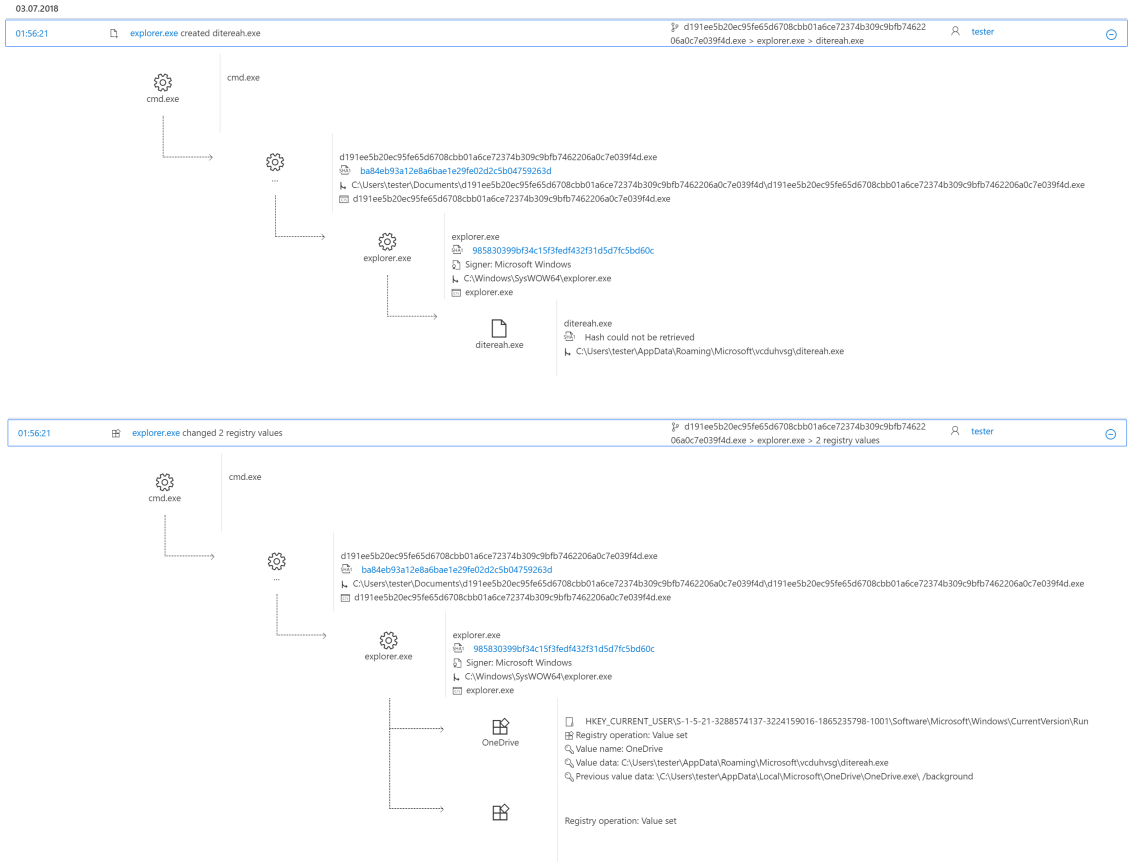


Figure 8. Windows Defender ATP alert process tree showing creation of new malware process (SHA-256: d191ee5b20ec95fe65d6708cbb01a6ce72374b309c9bfb7462206a0c7e039f4d) and registry modification

Command-and-control communication

Dofoil is an enduring family of trojan downloaders. These connect to command and control (C&C) servers to listen for commands to download and install malware. In the March 6 campaign, Dofoil's C&C communication involves the use of the decentralized Namecoin network infrastructure .

The hollowed *explorer.exe* process writes and runs another binary, *D1C6.tmp.exe* (*SHA256: 5f3efdc65551edb0122ab2c40738c48b677b1058f7dfcdb86b05af42a2d8299c*) into the *Temp* folder. *D1C6.tmp.exe*

then drops and executes a copy of itself named *lyk.exe*. Once running, *lyk.exe* connects to IP addresses that act as DNS proxy servers for the Namecoin network. It then attempts to connect to the C&C server *vinik.bit* inside the NameCoin infrastructure. The C&C server commands the malware to connect or disconnect to an IP address; download a file from a certain URL and execute or terminate the specific file; or sleep for a period of time.

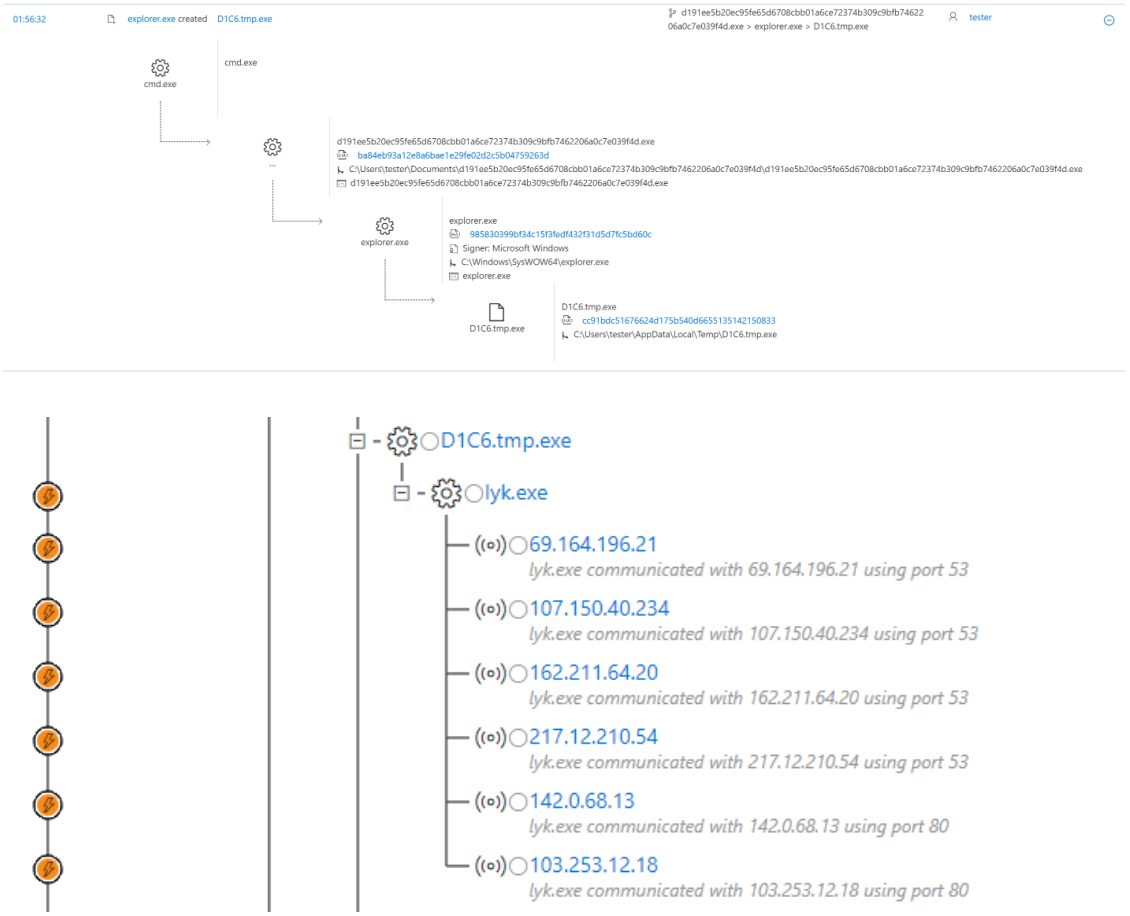


Figure 9. Windows Defender ATP alert process tree showing creation of the temporary file, D1C6.tmp.exe (SHA256: 5f3efdc65551edb0122ab2c40738c48b677b1058f7dfcdb86b05af42a2d8299c)Figure 10. Windows Defender ATP alert process tree showing lyk.exe connecting to IP addresses

Stay protected with Windows 10

With the rise in valuation of cryptocurrencies, cybercriminal groups are launching more and more attacks to infiltrate networks and quietly mine for coins.

Windows Defender AV's layered approach to security, which uses behavior-based detection algorithms, generics, and heuristics, as well as machine learning models in both the client and the cloud, provides real-time protection against new threats and outbreaks.

As demonstrated, Windows Defender Advanced Threat Protection (Windows Defender ATP) flags malicious behaviors related to installation, code injection, persistence mechanisms, and coin mining activities. Security operations can use the rich detection libraries in Windows Defender ATP to detect and respond to anomalous activities in the network. Windows Defender ATP also integrates protections from Windows Defender AV,

Windows Defender Exploit Guard, and Windows Defender Application Guard, providing a seamless security management experience.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Windows 10 S, a special configuration of Windows 10, helps protect against coin miners and other threats. Windows 10 S works exclusively with apps from the Microsoft Store and uses Microsoft Edge as the default browser, providing Microsoft verified security.

Windows Defender Research

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.

Follow us on Twitter @WDSecurity and Facebook Windows Defender Security Intelligence.
