WhisperGate: Not NotPetya

secureworks.com/blog/whispergate-not-notpetya

Counter Threat Unit Research Team

The WhisperGate wiper attacks in Ukraine may inspire memories of NotPetya, but there are significant distinctions. Security practices that mitigate ransomware attacks offer protection against WhisperGate. Friday, January 21, 2022 *By: Counter Threat Unit Research Team*
Destructive wiper attacks typically occur along geopolitical fault lines. Although some of these attacks masquerade as ransomware, there is a fundamental difference. Cybercriminals distribute ransomware to steal (or hold hostage) data that they can attempt to monetize. In

wiper attacks, the malware destroys data and renders it irretrievable. Wiper attacks are usually conducted by government-sponsored threat actors to serve political interests, not to generate profit.

Historical wiper attacks

The Shamoon wiper attacks in 2012, 2016, and 2017 were Iran's response to perceived regional adversaries. North Korean wiper attacks on South Korean organizations mirrored the military conflict between those countries. Even the 2014 attack on Sony Pictures Entertainment was retribution by North Korea against a movie studio for perceived offense against a political leader. Russian wiper attacks targeting Ukraine in 2015 and 2016 were followed by the infamous 2017 NotPetya attacks. While it's unlikely that the NotPetya threat actors intended its global impact and financial costs, it's clear they intended the malware to have a significant impact to Ukraine.

WhisperGate versus NotPetya

The WhisperGate wiper deployed in Ukraine on January 13, 2022 was another example of an attack serving political interests. WhisperGate is not a wiper-worm like NotPetya or WCry (also known as WannaCry). It doesn't have the SMB-based propagation mechanisms that made those worms so successful at spreading. The threat actors deliberately deployed WhisperGate to targeted organizations.

One reported attack vector used to deploy WhisperGate was a supply chain attack against a technology service provider. Details are limited as of this publication, but available evidence suggests that the supply chain attack involved a traditional compromise of the service provider. The threat actors then likely leveraged credentials and accesses from the provider's network to compromise its customers.

In contrast, NotPetya was delivered indiscriminately via a more sophisticated supply chain attack involving an accounting software provider. The threat actors used the legitimate software update mechanism to distribute and execute a weaponized update. NotPetya wormed its way across networks, rapidly escaping the intended geographic confines of Ukraine to infect networks and organizations globally.

Similarities between WhisperGate and ransomware attacks

Some of the tactics and attack vectors used in the WhisperGate attacks are similar to those used in ransomware attacks:

- Ransomware is often deployed to targeted organizations directly, just as WhisperGate was deliberately deployed to victims.
- Secureworks® Counter Threat Unit™ (CTU) researchers have observed threat actors compromising service providers to deploy ransomware.

- Some organizations impacted by website defacements likely associated with the WhisperGate attacks were reportedly compromised via exploitation of internet-facing vulnerabilities. Cybercriminals and government-sponsored actors quickly attempt to weaponize newly disclosed vulnerabilities.

Recommendations

Organizations with operations in Ukraine should be extra vigilant and review business continuity and resilience plans. It is unlikely that WhisperGate will impact organizations that are outside of Ukraine and are not connected to the geopolitical tensions in that region. However, organizations such as business partners and service providers in Ukraine that have logical access to customer networks should consider the potential for collateral damage that could spread to global operations.

For most organizations, ransomware is a more prominent threat. Cybersecurity practices to address ransomware attacks also provide significant protection against a WhisperGate-style attack:

- Maintain backups of business-critical systems and data, protect the backups from a potential ransomware or wiper attack, and regularly test restoration processes
- Develop a plan to continue operations during a power failure or loss of business-critical services
- Segment networks and limit access to high-risk areas
- Keep systems and software up to date, including applying patches for known vulnerabilities as soon as possible on internet-facing systems and leveraging antivirus solutions
- Implement endpoint detection and response solutions and investigate alerts of anomalous activity

For more details about WhisperGate, read the accompanying blog post about the attacks in Ukraine.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team. For other questions on how we can help, use our general contact form.