Operation Escalation: How click-fraud malware transforms into an advanced threat

cybereason.com/blog/how-click-fraud-commodity-malware-transforms-into-an-advanced-threat

Written By
Israel Barak

DON'T BE SO QUICK TO DISMISS LOW-LEVEL THREATS

Cybereason research clearly shows that companies should not be so quick to dismiss low-level threats. While the common belief is click-fraud malware, adware and similar programs annoy users but pose a relatively minor threat, we've seen several non-targeted commodity threats evolve into more dangerous and complex programs. In the cases our research team observed, including an incident that impacted a Fortune 500 company, these enhanced programs functioned as remote access tools and carried out malicious actions in addition to flooding a person's browser with ads or conducting click-fraud campaigns. **We named this process Operation Escalation.**

DETECT WHILE THE ATTACKERS ARE STILL UPGRADING

Detecting Operation Escalation early when a non-threat actor is still upgrading the commodity malware allows an enterprise to shut down the incident before the access is sold to an advanced threat group, which could carry out much more malicious activity.

Our research suggests that:

- Cyber-crime groups are getting better at analyzing where their broadly distributed malware has been installed, and identifying corporate environments that have high-value assets.
- Many commodity malware tools have broad remote tasking capabilities, providing their operators with a wide range of options to upgrade their capabilities, based on the initial infection location.
- Cyber criminals are looking to monetize higher value assets already installed in a corporate environment, typically by selling them to an organization with more targeted needs like a nation-state, groups engaged in financial cyber-crime or gathering business intelligence and hacktivist gangs.

COMMODITY THREATS ARE NOT THAT INNOCENT

In the incidents reviewed by Cybereason, the attack originated with click-fraud malware, adware or some other commodity malware infecting a company's machines. Kovter, a well-known malware, was used in a majority of the infections Cybereason observed, including several cases of our Fortune 500 customers.

In one incident that stands out for how quickly the asset was prepared for sale, Cybereason detected Kovter click-fraud malware on 10 computers in our customer's IT environment. Initially, the malware didn't display any behavior that was atypical for the program.

But a few days after the initial detection, Cybereason observed that the malware's behavior had changed in one computer: **Instead of communicating via a standard command and control network, the hackers had re-programmed the malware to communicate by using domain generation algorithms.** DGAs are more difficult to detect and offer a superior, more advanced way for attackers to communicate with their tools. Adding DGA communication abilities transformed the malware to a more sophisticated remote access tool capable of carrying out malicious activity without getting detected or blocked by traditional tools.

We suspect that the addition of DGA communication meant the attackers realized they had infiltrated a high-value target and were now especially interested in remaining undiscovered. Additionally, upgrading the click-fraud malware on only one computer allowed the hackers to probe the company's IT environment while decreasing the risk of getting caught.

At the same time the attackers added DGA capabilities, they also **re-programmed the malware to communicate with them only when the infected computer wasn't connected to the corporate network.** This enabled the malware to continue communicating with the hackers when the employee was using either a home or coffee shop

network. We suspect the attackers realized our customer was monitoring their communication with the malware, causing them to change their communication tactics to avoid placing the operation in jeopardy of being discovered.

The malware's persistence mechanism was also upgraded. The generic persistence mechanism was replaced with a more sophisticated one. The attackers used DLL side loading to load a fake Windows system file that looked and functioned like the authentic program but had additional capabilities. T**hey also added network and database scanning tools to the malware.**

At that point, eight days after Cybereason had detected the threat, the attackers stopped upgrading the malware. Typically, the hackers behind Kovter are focused on quickly making money through click fraud and other schemes. We assume they do not have an interest in exfiltrating data or carrying out an advanced persistent attack.

This doesn't mean another criminal group wouldn't be interested in executing this type of attack. In fact, we believe the hackers were preparing to sell this access to another criminal group. This would explain why they added more malicious capabilities to the malware, particularly functions that added persistence, nearly masked communication between the upgraded tool and the hackers and, overall, established an extremely strong grasp on the compromised machine.

HOW COMPANIES CAN DISCOVER OPERATION ESCALATION

With commodity threats having the potential to execute much more sinister activities, organizations may need to reconsider how they handle these programs. Security professionals can't disregard seemingly benign, unwanted programs that have infected their company's IT environment even though they're considered less of a threat compared to other security issues.

APT players just need one compromised machine to take over a company's entire network, just as in the Target breach. However, given the prevalence of adware, click-fraud malware and other commodity threats, organizations lack the staff, resources and time to investigate and remediate every infected machine.

Companies need a practical way to handle Operation Escalation. **Instead of removing all commodity programs, companies should diligently monitor them for behavioral changes and investigate those that act strangely.** Odd behavior, no matter how small, should not be disregarded. When changes to adware, malware and command-and-control traffic on infected systems are spotted, security teams should prioritize them to undergo further investigation and, when appropriate, remediation. For additional information on mitigating a Kovter malware infection, Microsoft published a blog with details on how to detect and remove this threat.

Spotting Operation Escalation offers a new way to protect against advanced attacks. An organization that can spot and remove common, low-level malware that's evolved into a malicious tool can block APT players from exploiting the affected machine and using it as an entry point into the company.

About the Author

Israel Barak

Israel Barak, Chief Information Security Officer at Cybereason, is a cyber defense and warfare expert with a background developing cyber warfare infrastructure and proprietary technologies, including that of proprietary cryptographic solutions, research and analysis of security vulnerabilities. Israel has spent years training new personnel, providing in-depth expertise related to cyber warfare and security, threat actor's tactics and procedures. As Cybereason's CISO, Israel is at the forefront of the company's security innovation, research and analysis of advanced threats.

All Posts by Israel Barak