BLOG
Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft
cybereason

Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation

Written By

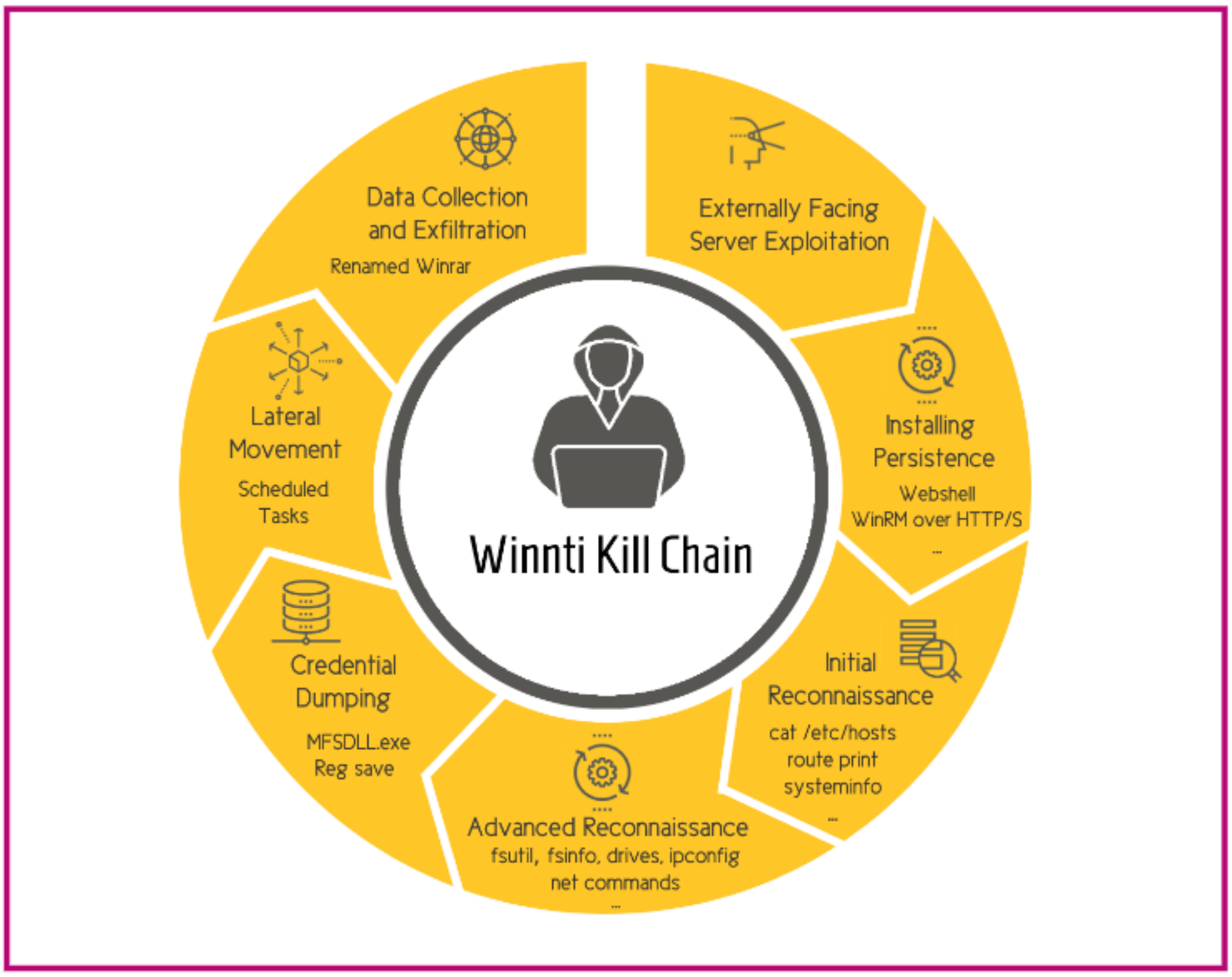
Cybereason Nocturnus

May 4, 2022 | 4 minute read

Cybersecurity often focuses on malware campaigns or the latest zero-day exploit. Surveys and reports reveal the average cost of a data breach or how much it typically costs to recover from a ransomware attack. Those are the attacks that make noise and capture attention, though. The attacks that fly under the radar are often more insidious and much more costly.

Researchers at Cybereason recently discovered such an attack, which was assessed to be the work of Chinese APT Winnti. Cybereason briefed the US Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) on the investigation into the malicious campaign, which Cybereason researchers dubbed Operation CuckooBees.

For years, the campaign had operated undetected, siphoning intellectual property and sensitive data. The team published two reports—one that examines the tactics and techniques of the overall campaign and another that provides a more detailed analysis of the malware and exploits used.



Winnti Kill Chain as observed in Operation CuckooBees

Operation CuckooBees

In 2021, the Cybereason Nocturnus Incident Response Team was engaged to investigate multiple intrusions targeting technology and manufacturing companies in North America, Europe, and Asia. They found an elusive and sophisticated cyber espionage campaign operating undetected since at least 2019.

With years to surreptitiously conduct reconnaissance and identify valuable data, it is estimated that the group managed to exfiltrate hundreds of gigabytes of information. The attackers targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data.

In addition, the attackers collected information that could be used for future cyberattacks, such as details about the target company's business units, network architecture, user accounts and credentials, employee emails, and customer data.

Cybereason researchers attribute the intrusions and Operation CuckooBees with a moderate-to-high degree of confidence to the Winnti APT group. Winnti, also known as APT 41, BARIUM, and Blackfly, is a Chinese state-sponsored APT group known for its stealth, sophistication, and focus on stealing technology secrets.

Key Findings

- Attribution to the Winnti APT Group: based on the analysis of the forensic artifacts, Cybereason estimates with medium-high confidence that the perpetrators of the attack are linked to the notorious Winnti APT group. This group has existed since at least 2010 and is believed to be operating on behalf of Chinese state interests and specializes in cyberespionage and intellectual property theft.

- Discovery of New Malware in the Winnti Arsenal: the reports expose previously undocumented malware strain called DEPLOYLOG used by the Winnti APT group and highlight new versions of known Winnti malware, including Spyder Loader, PRIVATELOG, and WINNKIT.

- Rarely Seen Abuse of the Windows CLFS Feature: the attackers leveraged the Windows CLFS mechanism and NTFS transaction manipulations, which allowed them to conceal their payloads and evade detection by traditional security products.

- Intricate and Interdependent Payload Delivery: the reports include an analysis of the complex infection chain that led to the deployment of the WINNKIT rootkit composed of multiple interdependent components. The attackers implemented a delicate "house of cards" approach, meaning that each component depends on the others to function properly, making it very difficult to analyze each component separately.

- The Winnti Malware Arsenal: the reports include an analysis of:

- ◦ Spyder: A sophisticated modular backdoor.

- ◦ STASHLOG: The initial deployment tool "stashing" payloads in Windows CLFS.

- ◦ SPARKLOG: Extracts and deploys PRIVATELOG to gain privilege escalation and achieve persistence.

- ◦ PRIVATELOG: Extracts and deploys DEPLOYLOG.

- ◦ DEPLOYLOG: Deploys the WINNKIT Rootkit and serves as a userland agent

- ◦ WINNKIT: The Winnti Kernel-level Rootkit.

- Multi-year Cyber Espionage Intrusions: The Cybereason IR team investigated a sophisticated and elusive cyber espionage operation that has remained undetected since at least 2019 with the goal of stealing sensitive proprietary information from technology and manufacturing companies mainly in East Asia, Western Europe, and North America.
- Newly Discovered Malware and Multi-Stage Infection Chain: the research examines both known and previously undocumented Winnti malware, which included digitally signed kernel-level rootkits as well as an elaborate multi-stage infection chain that enabled the operation to remain undetected since at least 2019.
- The Winnti Playbook: This research offers a unique glimpse into the Winnti intrusion playbook, detailing the most frequently used tactics, as well as some lesser-known evasive techniques that were observed during the investigation.

Winnti Group

The Winnti Group is one of the most prolific and successful threat actors in existence. Winnti has a history of attacks and campaigns supporting Chinese state-sponsored espionage activity and financially-motivated attacks.

Winnti is an exceptionally capable adversary. One report states, "The group's distinct use of supply chain compromises to target select individuals, consistent use of compromised digital certificates, and deployment of bootkits (rare among APT operators), highlight a creative and well-resourced adversary."

The Cybereason research agrees with that assessment. Operation CuckooBees offers a glimpse into the evolving Winnti intrusion playbook. Along with well-known and frequently used attacks, Cybereason researchers also witnessed unique evasive techniques.

Winnti leveraged both known and previously undocumented malware techniques, including digitally signed kernel-level rootkits. The threat employed an elaborate, multi-stage infection chain that was critical to enabling the group to remain undetected for so long.

Intellectual Property Under Siege

Intellectual property rights are essential to the global economy. Patents, copyrights, and trademarks are respected and enforced around the world because nations recognize that innovative concepts and the effort that goes into research and development and bringing them to market deserves to be rewarded.

It undermines the economy if other companies or nations steal intellectual property and force the originator to compete against their own innovation——often undercutting the price because they have no investment in research and development from which to recover costs.

Intellectual property is also a prime target for both corporate and nation-state espionage. Despite the agreements and protections in place, those with more ambition than ethics prefer to invest effort and resources in stealing the intellectual property of others rather than striving to develop their own innovations.

China and entities aligned with Chinese interests frequently engage in intellectual property theft. In May of 2021, the US charged four Chinese nationals for their involvement in a global computer intrusion campaign targeting intellectual property and confidential business information. The group employed fake online profiles and spear phishing, along with hijacked credentials and sophisticated malware to compromise networks and exfiltrate data.

Silent, But Costly

It is hard to determine the exact economic impact of intellectual property theft. There are a variety of factors involved. Data is the currency of business today, and the line between cyber espionage and nation-state espionage has blurred.

There are a variety of ways that stolen data might be used that could have significant consequences. Suffice it to say that losing gigabytes of sensitive and proprietary intellectual property is a massive hit to the bottom line and erases any competitive advantage in the marketplace.

It is also hard to estimate the exact number of companies affected by Operation CuckooBees due to the complexity, stealth, and sophistication of the attacks. Winnti is one of the most industrious groups operating on behalf of Chinese state-aligned interests.

Over the years, there have been multiple reports and US Department of Justice (DOJ) indictments tying Winnti to large-scale IP theft operations. Cybereason researchers believe that dozens of other companies were potentially affected by this or similar campaigns carried out by Winnti.

Cyber espionage doesn't usually generate the same degree of panic or media attention as other cyberattacks, but the lack of attention doesn't make it any less dangerous. A malicious campaign that silently steals intellectual property for years is exceptionally costly and may have repercussions for years to come.

The Cybereason Nocturnus Team has published two reports related to Operation CuckooBees. For more on this campaign and the tactics, techniques, and processes used, check out Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques. For a detailed look at the malware toolkit employed in Operation CuckooBees, check out Operation CuckooBees: A Winnti Malware Arsenal Deep-Dive.

Share

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus NEWSLETTER

Never miss a blog

Get the latest research, expert insights, and security industry news.

Subscribe