COMCAST BUSINESS | MASERGY

CASE STUDY

- Managed Detection & Response (MDR)
- Cloud Security
- Security Analytics
- SOC Services

Protecting against North Korean malware, finding a missing employee in Russia, and more Masergy security success stories

Work-from-home trends have given cybersecurity criminals even more opportunities, and today ransomware has increased by 148+%. As a result, every IT leader is thinking about the best ways to ratchet up security efforts. With three global Security Operations Centers (SOCs) analyzing more than 45 billion security events annually, Masergy stays on top of security threats for clients of all sizes. Using machine learning, behavioral analytics, and 20+ years of threat intelligence, our certified security analysts don't just monitor threats and craft a prioritized response plan, they also act on threats to actively defend clients 24/7.

Clients have recognized these benefits as a result of their Masergy services:

- Legal firm Weightmans LLP gains 144 hours in productivity every quarter
- Financial firm Intertrust tackles compliance with help from Masergy
- Without Masergy financial firm Elevate would have to add 3-4 more staffers to maintain a 24/7 security monitoring

Here are some more true client success stories detailing how Masergy's managed detection and response services averted security risks with the potential to create catastrophic damage. Craig D'Abreo, Masergy's VP of Global Operations, explains the significance of each attack and the best practices for counteracting them.

5 reasons to choose Masergy for security

1. One partner for technologies and analytics
2. 24/7 managed detection and response
3. Machine learning and behavioral analytics
4. Full network visibility for "east/west" site-to-site traffic monitoring
5. Pricing based on users, sites, and log sources

ROKRAT: Responding to North Korean malware

Customer: Higher education organization

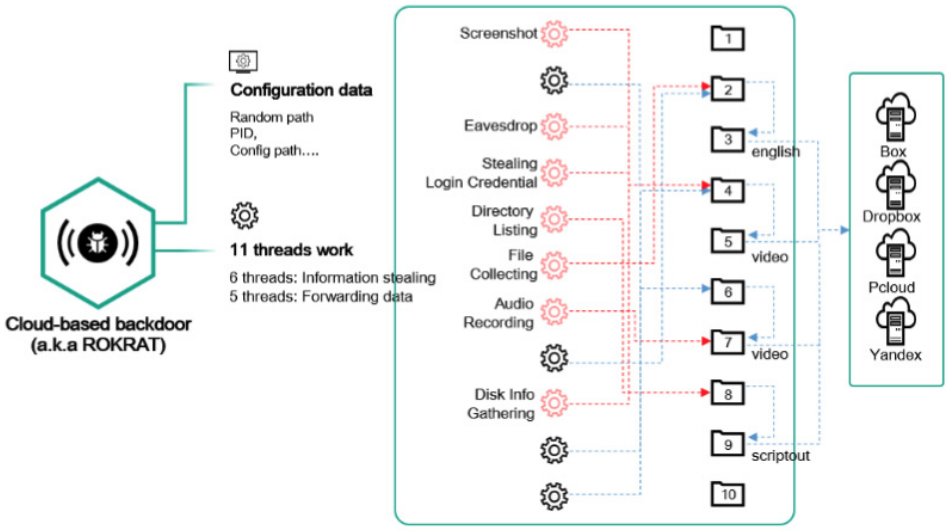
Threat: ROKRAT is a type of malware originating from North Korea. It's a malicious software designed to exfiltrate data, steal credentials, and capture screenshots from the infected corporate IT environment. Some of the latest variants of this malware use popular cloud applications and services such as PCloud, Dropbox, and Yandex as the channel through which the attacker commands and controls the infected system. This threat is used to:

- Implement a backdoor on the corporate network for future compromise
- Steal corporate information from the host and network
- Exfiltrate sensitive data from the company

Detection: By tracking the SSL certificates of the websites known to be hosting the ROKRAT trojan, Masergy's SOC was able to identify the threat and alert the client of the suspicious activity.

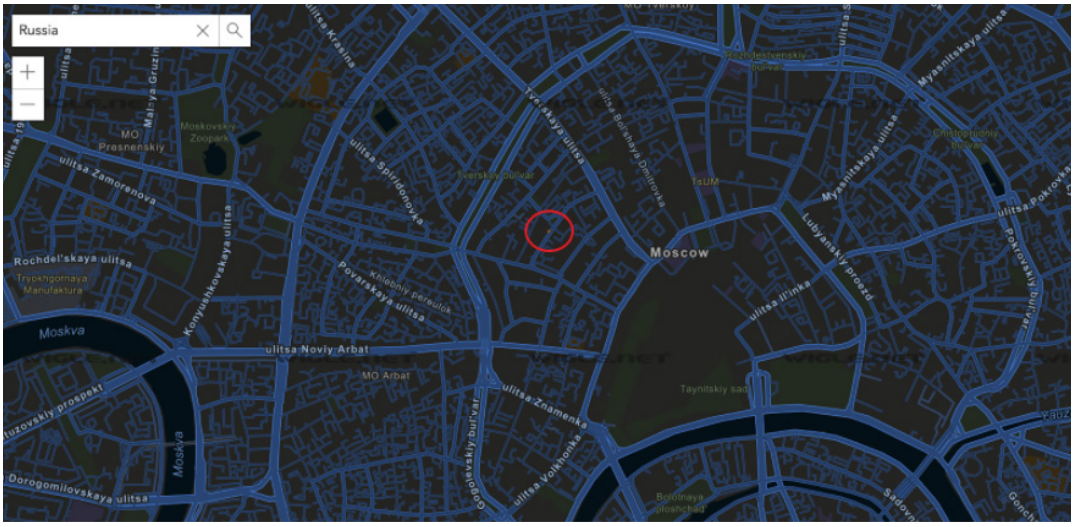
Investigation: Masergy's security team began correlating multiple data sources from the customer network infrastructure to confirm a ROKRAT attack. Further investigation proved a positive detection--the threat was real.

Response: Masergy's certified security analysts quarantined the device and prevented communication to other devices on or off the network.



"Some companies don't take malware and ransomware seriously, because they think their data has no value to bad actors. When in reality, attackers aren't picky about data. They don't always target high-value personal, financial, or medical data to resell. Instead, they try to get into any system, holding any corporate data hostage until you payout. Malware is a serious threat and can easily become a ransomware situation. Proactive prevention and 24/7 security monitoring is a must."

Craig D'Abreo
VP of Global Operations, Masergy



Using EDR to find a missing employee in Russia

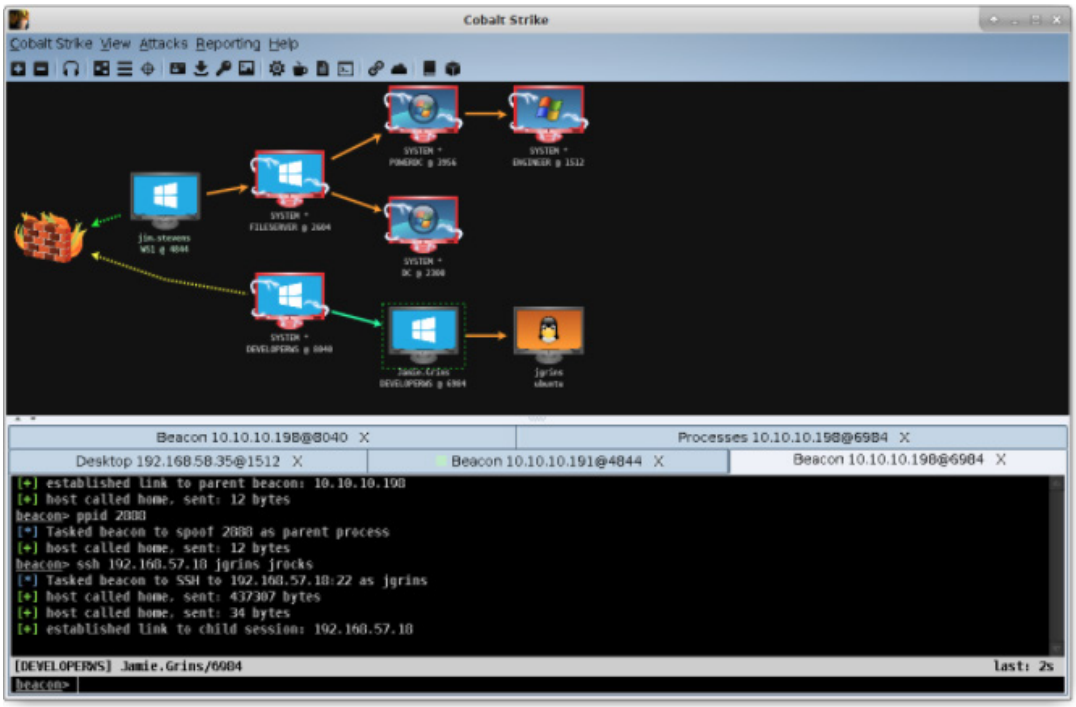
Customer: Financial Services Company

Threat: In the midst of the COVID-19 pandemic, an executive client called the Masergy SOC with an urgent request for help. An employee who had been travelling in Russia on business had gone missing. The client wanted help in using the employee's laptop computer as a means for tracking their location.

Detection, Investigation, and Response: Within 20 minutes, Masergy's security team made contact with the individual's laptop and then attempted to identify its exact location by creating a makeshift GPS. Within 40 minutes, Masergy had isolated its location within a 50-meter area in Moscow. The team used endpoint detection and response (EDR) technology in this effort, acquiring a list of nearby WiFi networks which were then combined with open source intelligence databases to contain geographic data. Within 60 minutes, the missing person was safe back in their apartment and reunited with their company contact in Russia.

"While this might sound like a segment out of a thriller movie, it's a true story and a great example of how Masergy can think outside the box to solve tough security challenges, acting as a true extension of the client's team."

Craig D'Abreo
VP of Global Operations, Masergy



Adverse effect: When bad actors use tools designed to do good

Customer: Transportation and Logistics Company

Threat: Cobalt Strike is a commercially available suite of software and tools originally intended to help companies identify potential threats. It's used for threat simulation during pen-testing exercises, but bad actors can also use it against you. "Cracked versions" exist and can be used to conduct attacks filelessly leveraging the device's memory system. This is what the Cobalt Strike vendor terms a "beacon."

Detection and Investigation: EDR technology triggered an alert, at which time Masergy's security team investigated it using correlation techniques with the client's available data sources.

Response: Masergy analysts and the client worked together to access detailed information on the processes running and to action to prevent recurrence.

"When threats like these use in-memory and fileless attack methods, traditional antivirus products will fail at detection. This proves why an EDR technology backed by a team of dedicated 24/7 security professionals is necessary today."

Craig D'Abreo
VP of Global Operations, Masergy

Kovter spam mail: Catching hard-to-detect fileless malware

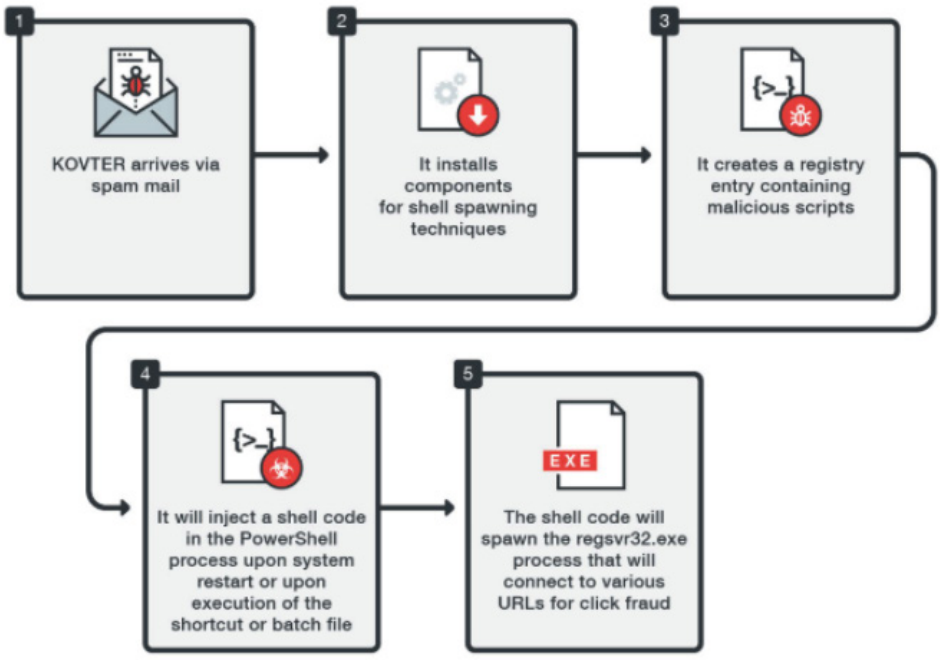
Customer: Law firm

Threat: Kovter is a constantly evolving piece of malware originally associated with ransomware and has since transformed into fileless malware, making it even harder to detect. Kovter works by embedding itself in the Windows operating system's registry to stay hidden. This allows the potential for nefarious activity, including:

- Backdoor access to a network and a gateway for additional malware
- Stealing personal information and corporate data from the host
- Exfiltration of sensitive data from of the corporate network

Detection and Investigation: The client's Masergy monitoring console alerted to a malicious backdoor. This particular alert indicates that an SSL certificate, known to be utilized by Kovter, had been downloaded. This told Masergy to investigate further. In investigating the threat, its characteristics matched the key markers or footprints of the Kovter malware family.

Response: Masergy analysts and the client worked together to access detailed information on the processes running and to action to prevent recurrence.



"This threat was introduced via a spam email. Phishing is still a big risk for companies and what many may not realize is that phishing can easily turn into malware and ransomware attacks. Ransomware attacks have been incrementally increasing by 148+% year over year and can cost companies millions of dollars. No matter how much you educate employees on cybersecurity risks and trust them to protect their devices and endpoints, ransomware attack methods are continuously evolving, and endpoint deficiencies are often the primary reason organizations fall victim to ransomware attacks."

Craig D'Abreo
VP of Global Operations, Masergy