Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY:

Redline Infostealer

Malware Attack That Steals User and System Information

Redline Infostealer is a malware family that is known to steal and exfiltrate a target victim's data. It collects information about the user and their system including the username, location, hardware configuration, and installed security software. It can also steal saved login credentials, cryptocurrency wallets, credit cards, cookies, and autocomplete fields from browsers. It is often distributed by phishing email campaigns but can also be delivered by other methods, including tools and games.

Trinity Cyber recently prevented a Redline Infostealer attack in real time on live customer traffic. The attack was exposed and prevented in the early stages before data was lost. Trinity Cyber thwarted this attack on a U.S. university's network used by faculty, staff and students.

Repeated Attempts Defeated Every Time

Trinity Cyber's Analysis team first detected Redline Infostealer in the early stages of the attack by the content of its command and control (C2) traffic. A student's computer was unknowingly infected with Redline malware, and as it attempted to beacon from inside the university network out to a C2 server, it was identified and stopped by the Trinity Cyber Engine. Because the attack was detected and neutralized in the early stages, no data was exfiltrated from the device. This malware attempted over 1,600 beacons after it was first prevented, retrying its connection frequently. Although this exploit successfully evaded other security infrastructure technologies, it was prevented each time by the revolutionary Trinity Cyber Engine.

As a result of Trinity Cyber's rapid engagement with the SOC team, the university acted swiftly to identify, locate and isolate the infected laptop from the campus network within 10 minutes. The infected device belonged to a student who was quite surprised to learn it was infected and a potential source of harm to the university.

KEY TAKEAWAYS

- **Identified and stopped a malicious threat coming from inside the university network**
- **Intercepted and defeated a persistent C2 attack**
- **Protected the university's students and faculty with automated actions, not just alerts**
- **Defeated malware missed by other deployed security infrastructure**
- **Expanded network visibility**
- **Reduced SOC staff workload**
- **Happy customer, frustrated adversary**

The Revolutionary Trinity Cyber Engine

The Trinity Cyber Engine is tuned to defeat attacker tactics, techniques and procedures (TTPs) at multiple stages to protect networks against entire classes of actual malware, command and control (C2), remote exploits, drive-by downloads and in-the-wild malicious threats and techniques that are commonly missed by traditional detect-and-respond systems. The technology is unique in its ability to deeply inspect full session Internet traffic —at line rate speed and in both directions—to expose and mitigate threat content inline. It combines near-zero False Positive Rate accuracy and depth (providing rich contextual application layer fidelity) with automated preventive controls that protect networks from threats and are executed with an average latency of < 1ms.

Want to learn more about how you can benefit from this powerful solution? Reach out to Trinity Cyber at info@trinitycyber.com for more information.

Gartner
COOL
VENDOR
2020