Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY:

OSX.pirrit (Adware)

A Multi-stage, Malicious, Command and Control (C2) Attack

OSX.pirrit adware targets Mac OSX and can often be used for nefarious purposes. It establishes persistence and includes capabilities that obtain root access. It is known to take complete control of a user's machine while simultaneously making it very difficult for the user to remove it.

Trinity Cyber recently identified a multi-stage command and control (C2) attack with a malware variant of OSX.pirrit across our live customer traffic, signaling a strong indication this attack was more than benign adware. Trinity Cyber thwarted this attack on a U.S. university's network used by faculty, staff and students.

Attack and Subsequent Attack...Defeated

Trinity Cyber's unique technology detected low volume C2 traffic that was evading existing firewall, IPS and EDR defenses. This variant of OSX.pirrit beacons outbound to its C2 controller for a payload. Trinity Cyber examined the payload, rapidly identified and thwarted a second stage Mach-O file and an evasive malware that targets MacOS 64-bit computers. This malware is designed to provide root-level access to deliver targeted adware and malicious payloads.

Trinity Cyber identifies and stops OSX.pirrit malware at multiple stages of attack. In the case of this university customer, shortly after stopping the first stage of attack, we discovered that the adversary was actively working to evade our first stage prevention measures while we were simultaneously actively preventing the second stage of the attack. These moves and counter moves are a strong indication that this attack was part of a larger campaign and a good example of how Trinity Cyber's revolutionary approach to protection frustrates attackers while keeping customers protected. This attack, which successfully evaded existing defenses, was detected and defeated by the patented Trinity Cyber Engine.

KEY TAKEAWAYS

- **Identified and stopped a malicious threat**
- **Intercepted and defeated a multi-stage C2 attack**
- **Protected the university's students and faculty with automated actions, not just alerts**
- **Delivered protection missed by other technologies in place**
- **Expanded network visibility**
- **Reduced SOC staff workload**
- **Happy customer, frustrated adversary**

The 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