PONDURANCE

INCIDENT RESPONSE

DIGITAL FORENSICS AND INCIDENT RESPONSE

Digital Forensics and Incident Response (DFIR) is an evolving challenge that requires a combination of tools, methodologies and people to execute successfully. Pondurance is committed to maintaining the most qualified DFIR workforce with subject matter experts that have over a decade of experience in responding to cyber security incidents. Our experts train year round to respond to threats by obtaining professional credits, attending premiere security events, and leading research and development of new tools and techniques. Pondurance experts utilize existing tools such as FTK and Volatility while having the ability to quickly build custom capabilities based on the needs of our clients. Sustaining a premiere work force in addition to tools and methodologies allows Pondurance to remain ready to conduct fast and effective incident response investigations at any moment.

THE PONDURANCE TEAM REGULARLY DEALS WITH

- Denial-of-Service Attacks
- Malware Infection (Ransomware)
- Advanced Persistent Threats
- Phishing Attempts
- Unauthorized Root/Admin Access
- Data Exfiltration
- Post-Breach Analysis
- Incident Command
- Disk, Memory and Network Forensics
- eDiscovery

THINK YOU'VE BEEN BREACHED? | 317.663.8694

PONDURANCE

OUR EXPERIENCE WITH DFIR

SAMSAM RANSOMWARE //

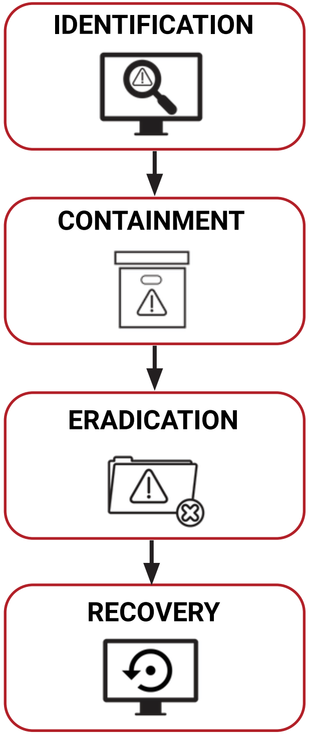
SamSam Ransomware involves manual entry onto the target network, with patience for privilege escalation and precise mapping of the network's infrastructure. These actors work efficiently and effectively to encrypt as much data as possible on the network, thus rendering affected data inaccessible. Following encryption, these actors calculate customized payment amounts depending on assumed criticality and quantity of affected systems.

EMAIL PHISHING OUTBREAK //

Despite efforts to implement various forms of Multi-Factor Authentication, the tactic of targeting users over false emails continues. Recently, the most effective tactic involves sending mass-emails to a compromised user's entire address book. At this point, attackers can identify internal users involved in payroll and accounting where they then work towards currency acquisition from both internal and external sources.

WANNAMINE "CRYPTOMINER" //

The capabilities of this persistent crypto-miner, including self-propagation via credential theft, exploits, privilege escalation, and credential-exfiltration, go far beyond the typical crypto-mining malware. Additionally, this malware prefers to max out CPU at 100% while also terminating other processes competing for resources, thus eliminating the availability of affected systems to perform intended functionalities. The consistent exfiltration of stolen credentials performed by this malware complicates the situation further, as the door for reentry into the network post-recovery must be addressed.



IDENTIFICATION

CONTAINMENT

ERADICATION

RECOVERY

THINK YOU'VE BEEN BREACHED? | 317.663.8694