CYLANCE CONSULTING

Ransomware Prevention & Remediation

Don't be the next victim

This threat:

- Does not typically rely upon traditional spear phishing or watering hole attack vectors
- Leverages vulnerable externally facing services so bad actors can manually move laterally and establish persistence
- Can canvas and encrypt entire networks instead of just a handful of individual hosts
- Targets backup systems within the net work and deletes archives instead of just encrypting them, leaving victims little to no recourse[1]

The SamSam (aka Samas, or Samsa) ransomware is a new generation of ransomware that is not industry specific.

[1] *FBI FLASH MC-000070-MW distributed by the FBI to specific entities (TLP:GREEN) on March 25, 2016.*

Current Ransomware Threat Environment

Today's ransomware campaigns are very different from what we have seen in the past. On the one hand, ransomware can be easily obtained and used successfully by criminals that have little to no hacking skills, often referred to as Ransomware as a Service (RaaS). On the other hand, we are seeing ransomware being used for much more than just ransoms. In some cases, we have seen it used as a diversion; first harvesting credentials for later use, and then encrypting the drive to keep IT staff occupied while the attacker covers their tracks and accomplishes even more nefarious objectives. And more recently, we are seeing highly opportunistic campaigns that encrypt entire networks in an organization and delete host backups prior to encryption, leaving the entire organization held hostage and unable to operate.

Cylance® offers two complementary service offerings to help organizations address this evolving threat.

Proactive Prevention and Readiness

Cylance offers best practices for prevention, network architecture, internal IR workflows, vulnerability and patch management, and assessment of both internal hosts and externally facing services that criminals are using to gain foothold.

When it comes to ransomware, prevention and preparation are the best medicine. Once execution takes place, the business cost and business risk go up exponentially. Likewise, organizations that are well prepared for ransomware can greatly minimize the business impact of an IT incident in general.

Cylance's Proactive Prevention and Readiness services cater specifically to the ransomware epidemic by:

- Leveraging the power of machine learning and artificial intelligence to allow predictive, autonomous, pre-execution prevention
- Providing world-renowned, highly sought after, knowledgeable consultants with the expertise to facilitate remediation of a ransomware attack
- Imparting wisdom BEFORE the attack occurs to ensure the best preparation, preventative technologies, and workflows are in place

Related services and products

Industrial Control Systems

- ICS Infrastructure Assessment
- ICS Compromise Assessment
- Building Automation Systems
- Incident Response Services for Control Systems

Internet of Things /Embedded

- Incident Response for IoT and Embedded Systems
- Penetration Testing for Embedded Systems

ThreatZERO™

- ThreatZERO + Compromise Assessment
- ThreatZERO Resident Expert

Healthcare

- Clinical Information Security Program Development
- Clinical Application Security Assessments
- Medical Device Risk Assessment
- HIPAA Compliance

Training

- Custom Incident Response and Forensics Training
- ICS Security Essentials Incident Response and Compromise Assessment
- Malware and Incident Response Retainer Services
- Incident Readiness Assessment
- Emergency Incident Response

Enterprise Security Services

- Internal / External Penetration Testing
- Social Engineering
- Web Application Assessment

Incident Response, Rapid Containment and Risk Reduction

Not all ransomware is created equal. As soon as one variant is released, a host of 'copy-cat' variants emerge, and some of them use entirely different encryption algorithms and key-exchanges, while others still, use new command and control infrastructures or different attack vectors. In the unfortunate case an organization needs to call in IR services, it is important to demand experienced responders armed with a structured process and custom-built tools so these types of determinations can be made quickly in order to move to rapid containment.

The Cylance IR team has conducted hundreds of IR engagements just this last year alone. They are experts in hunting for key indicators of compromise for current active campaigns and are able to directly leverage Cylance's machine learning and artificial intelligence engine for immediate containment during the IR process, all without installing any agents or tipping their hat to the criminals behind the campaign.

The goal during any ransomware compromise is the same: reduce the risk and cost to the organization, and restore operations as soon as possible; all while moving silently, quickly and purposefully.

Cylance Consulting is focused on immediate containment without a managed service provider commitment or agents left on your network. We eliminate the vulnerability and prevent it from further exposure, permanently. We challenge you to find an organization that can contain incidents faster and prevent them from occurring in the future.

Cylance's Incident Response, Rapid Containment and Risk Reduction of ransomware compromises provides:

- Experts in the space who have completed hundreds of IRs per year
- Custom-developed tools to specifically address today's advanced ransomware
- Structured and proprietary response workflows to rapidly identify and contain the campaign
- Ransomware analysis to determine if certain aspects are breakable in order to possibly defeat the need to pay ransom
- Assistance in negotiating with criminal actors behind attack campaigns during late-stage attack campaigns
- The benefits of artificial intelligence without the need to install a host-based agent, which can tip off the criminals behind the campaign

+1-877-97DEFEND
proservices@cylance.com
www.cylance.com/consulting
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™

20160623-1271