CASE STUDY

CryptoLocker Ransomware Infection

Defense Contractor solves ransomware infection and gains reassurance of complete and continuous visibility over potential operational risks.

Industry
Defense Contractor

Challenge
Eliminate ransomware infection and prevent future reoccurance

Environment
One server room with 150 endpoints deployed with anti-virus, webfilters, and IDS/IPS solution

Results
1. Recovered and restored business operations in just hours
2. Gained deep visibility into origin of the attack and status of all endpoints
3. Saved hours of time and associated costs

INTRODUCTION

A mid-sized defense contractor found itself the victim of a relatively new variant of a cyber-attack, called CryptoLocker. CryptoLocker is a variant of a ransomware trojan targeting computers running Microsoft Windows. CryptoLocker propagates via email attachments, or simply by an end-user surfing the internet. It can strike at any time. When active, CryptoLocker encrypts all files stored on local and mapped network drives making it virtually impossible to reestablish the original content, without the ransom paid in bitcoins to an anonymous account.

CryptoLocker subverted the contractor's existing security controls, including internal IDS/IPS, webfilter gateway, and antivirus endpoint protection entirely due to the zero day nature of the ransomware variant.

RANSOMWARE VARIANTS:

Cyrptolocker, CryptoWall, TorrentLocker, Gameover ZeuS, TeslaCrypt, Linux.Encoder.1, Filecoder.A, Trojan. Linux.Ransom.A

> *"41% of those who claimed to be victims said that they decided to pay the ransom, as they could not adequately recover files which had been backed up. It is believed the ransomware extorted a total of around $3 million."*
>
> -Researchers at the University of Kent

PROTEUS TECHNOLOGIES | 133 National Business Parkway, Suite 150 | Annapolis Junction, Maryland 20701
WWW.PROTEUS-TECHNOLOGIES.COM/CYBERVIGILANCE | CV@proteuseng.com

SOLUTION

RESEARCH: INCIDENT MANIFESTATION

PROTEUS' CyberVigilance™ solution was able to discover the infection before it encrypted many of the files on the defense contractor's corporate network. Initial detection occurred when alerts of increased anomalous and external traffic were seen in the CyberVigilance™ Operations Center (CVOC). Additionally trouble tickets were beginning to hit the helpdesk as employees were beginning to notice out-of-place files while reviewing documents on their file shares.

REMEDIATE: INCIDENT CONTAINMENT

To contain the damage caused by CryptoLocker, the CVOC immediately contacted the company's IT staff and requested for them to temporarily shut down internal network access. This measure was enacted in order to prevent the spread of the ransomware, stop the encryption of files on the network shares, and to prevent any additional outbound command and control activity.

This action immediately stopped the anomalous traffic allowing CVOC engineers to begin the investigation of the incident. Leveraging several of the centralized logging and analytic tools that are part of the CyberVigilance™ solution, CVOC engineers were quickly able to pinpoint the source of the infection.

RESPOND: INCIDENT RESPONSE AND RESTORATION

The investigation revealed a single infected computer system. The offending workstation was physically removed from the network and quarantined for future analysis.

At that point PROTEUS' CVOC engineers worked directly with the company's IT staff to meticulously scan every system connected to the network to ensure that the CryptoLocker ransomware or any other variants were contained and removed if discovered. Once the scans were completed, it was determined that the CyberVigilance™ solution provided the evidence needed to ensure that 100% of the attack had been contained and remediated.

Following containment, network access was restored and the company's IT staff began their internal process of restoring files from backup, and tightened web-filter protocols.

RESULTS

Within two hours of the CyptoLocker attack first being identified, CyberVigilance™ engineers remediated and restored all files, network traffic, and briefed senior management on the event. The defense contractor was back to business thanks to CyberVigiliance™.

PROTEUS TECHNOLOGIES | 133 National Business Parkway, Suite 150 | Annapolis Junction, Maryland 20701
WWW.PROTEUS-TECHNOLOGIES.COM/CYBERVIGILANCE | CV@proteuseng.com

CONCLUSION

It is critical to continuously monitor and alert on suspicious network activity, as in this example, on the creation of filenames associated with malware or renaming of large numbers of files in a short time.

Using CyberVigilance™, the company was reassured that had complete and continuous visibility over the potential operational risks security threats post to their internal systems. CyberVigilance™ enabled the company to restore network access and business operations much faster than had they analyzed data using traditional methods.

> *"CryptoLocker's creators are almost certainly seasoned in malware campaigns that appear to have made sound design decisions that complicate efforts to mitigate this threat and have demonstrated a capable distribution system based on the Cutwail and Gameover Zeus botnets."*
>
> -Dell SecureWorks

CyberVigilance™

A PROTEUS TECHNOLOGIES CYBER SOLUTION

#ACTB4URHACKD

RESEARCH + **REMEDIATE** + **RESPOND**

About PROTEUS Technologies

PROTEUS Technologies, LLC (PROTEUS), is a leading provider of high-end Cyber Solutions, SIGINT and Technology, Research & Innovation, and Embedded Engineering software services to the Intelligence Community, Federal Executive Departments, HealthCare, and Commercial Industries. PROTEUS has a proven track record of excellence and commitment to client mission success. PROTEUS Headquarters is located in Annapolis Junction, MD with satellite offices in Columbia, MD, and is the 2010 winner of the prestigious DoD Nunn-Perry Award winner, multiple annual Baltimore Business Journal "Best Places to Work" awards, and the most recent Corporate America Software & Technology Award Winner for Innovation in Software/Systems Engineering.

PROTEUS TECHNOLOGIES | 133 National Business Parkway, Suite 150 | Annapolis Junction, Maryland 20701
WWW.PROTEUS-TECHNOLOGIES.COM/CYBERVIGILANCE | CV@proteuseng.com