



Edge.

THE REGION'S NONPROFIT TECHNOLOGY PARTNER

Scottish Rite CyberSecurity

Presented by: Jeremy M. Livingston
Presented on: 9/12/2019

Bio: Jeremy M. Livingston

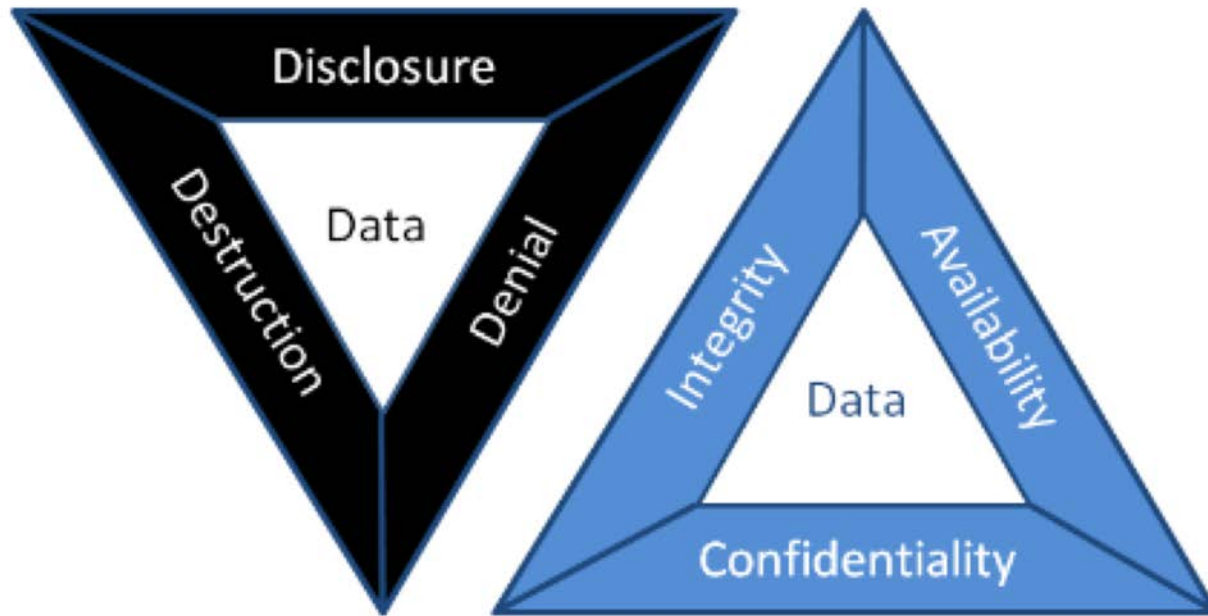
- CISSP, Security+, MCSE
- Masters in Cybersecurity
 - Current Doctorate student
- AVP & CISO NJ Edge
- vCISO at Fairleigh Dickinson University
- Security Advisor to Rutgers
- Senior Partner – Fortium
- CISO at Food & Drug Administration
- CISO at Federal Housing Finance Agency
- Security Manager - NASA Goddard
- Cyber Risk Manager - National Nuclear Security Agency
- Senior Information Security Analyst – Executive Office of the President, The White House
- US Navy Veteran
- Junior Warden of Patmos-Solomon's #70 in Savage MD





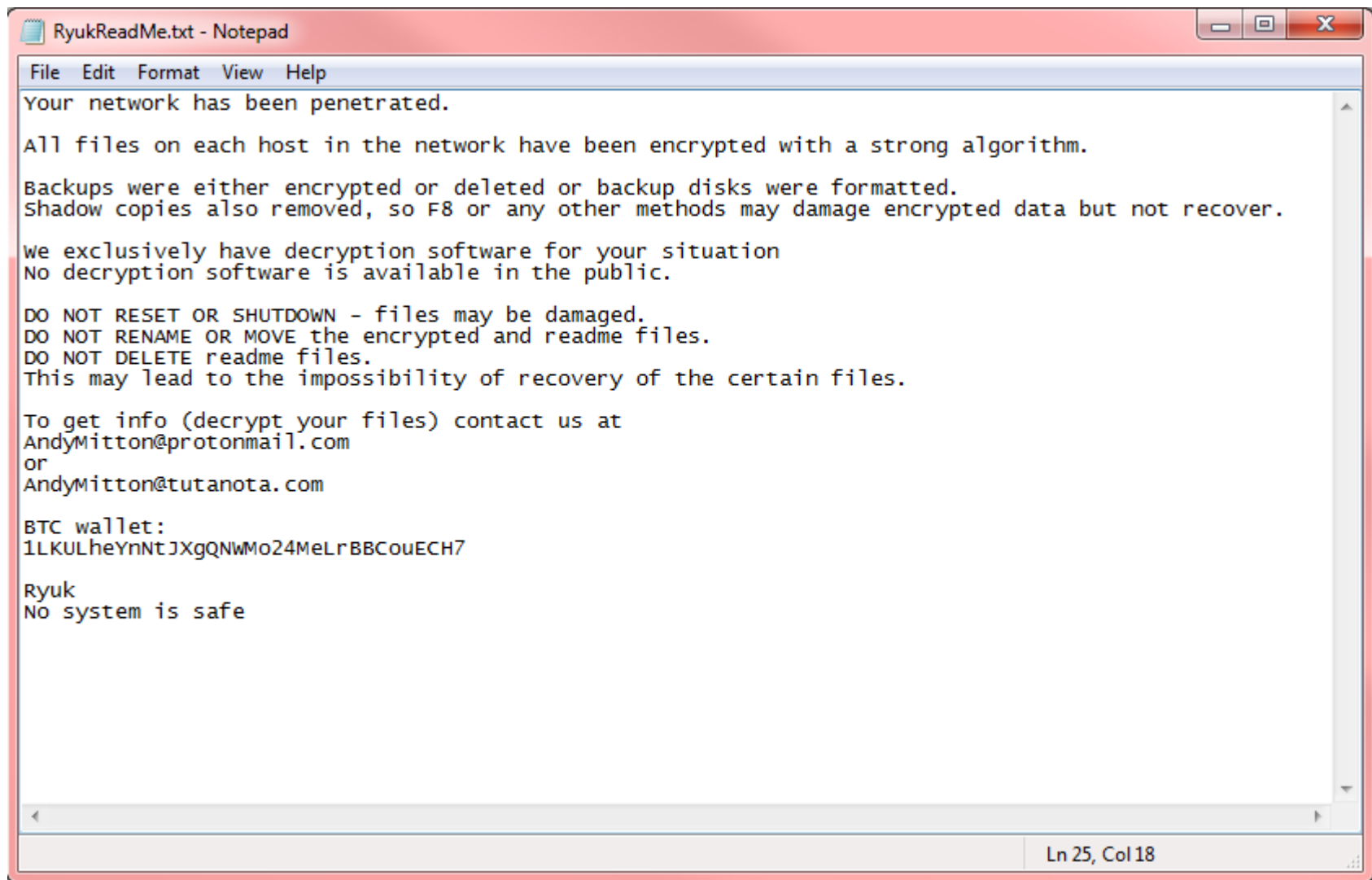
What is a Cyber Risk?

Vulnerability + Threat = Risk



Types of attacks

- Ransomware
 - Advanced Ransomware w/ data exfiltration
- Phishing/spear-phishing
- Spoofing
- Drive-by



RyukReadMe.txt - Notepad

File Edit Format View Help

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNwMo24MeLrBBCouECH7

Ryuk
No system is safe

Ln 25, Col 18

Recent Attacks

- Wallenpaupack Area School Districts
- Stevens University
- Regis University
- Monroe College
- City of Tyler TX
- Lake City FL
- Riviera Beach FL
- Baltimore City MD
- Cockrel Hill TX
- Sarasota FL
- Entercom Media Corporation
- Texas Department of Information Resources
- Flagstaff AZ School District
- Regis University

How do we protect ourselves?



Preventative Measures

- Audit your network for external-facing remote desktop protocol (RDP) and terminal services and turn them off where possible. If you cannot turn the services off, ensure they are patched, enable two-factor authentication, and change the default ports. Limit RDP access to only those users who have a business need for it, and secure access through a virtual private network (VPN) or Remote Desktop gateway.
- Enable strong passwords and account lockout policies to defend against brute-force attacks. Log and monitor RDP logins and attempted logins.
- It is a best practice to turn on two-factor authentication for external access to all applications. This is particularly true for sensitive ones such as email, payroll, or benefits providers, RDP, and VPNs.
- Ensure anti-virus software is up-to-date. Use a separate password to protect anti-virus settings.
- Regularly train employees to avoid phishing attempts and not to open unsolicited attachments and links, particularly from unknown sources.
- Periodically test employees through phishing campaigns, monitor the effect on response rates, and consider formal sanctions policy (after consultation with HR and legal counsel) for repeat offenders.

Preventative Measures 2

- Block emails with .jl, .wsf, and .zip extensions and macros at your email gateway level. If possible, disable the following commonly used attack vectors: Adobe Flash Player, Java, and Silverlight.
- Block macro-enabled malware files from running on Microsoft Office programs like Word, Excel, or PowerPoint by using group policy settings.
- Disable SMBv1 on all Windows systems.
- Disable Powershell on workstations.
- If you use Jboss, review the developer information on configuring and hardening it.
- Evaluate whether application whitelisting makes sense for your systems.
- Disable autorun/autoplay functionality on your OS to prevent malicious software from running on your computer.
- Enable automated patches for OS and browsers where possible.
- Robust network segmentation can reduce the impact/spread of ransomware.
- Enable strong identity and access management, with the of established principles of least privilege (“need to know”), and limit local administrative rights.

Preventative Measures 3

- IDS/IPS to monitor signs of malicious activity.
- Implement (and test) a data backup and recover plan to maintain copies of sensitive or proprietary data in a separate and secure location (offline if possible). Backup copies of sensitive data should not be readily accessible from local networks.
- Run advanced endpoint protection software. This can prevent the infection, or help detect the infiltration as it is happening.
- Some type of DNS cleansing service (ransomware reaches out to a command and control (C&C) server for encryption keys etc).
- Advanced Firewalls with automatically updated block lists (many ransomware programs will fall back to a hard-coded IP if the DNS lookup fails).
- Have contracts in place with needed vendors prior to an incident. Whether it's hardware replacement or surge capacity for the increased workload, you won't have time in the middle of an incident and you won't get the best rates.
- *** USER TRAINING *** the most effective defense is an engaged and knowledgeable workforce who know what to look for



Questions/Comments/Discussion

Contact:

Jeremy M. Livingston

jeremylivin@gmail.com

202-230-2947 (mobile)