Securing Tomorrow
Ransomware

Trevor Richmond June, 2016
CANHEIT 2016
Ransomware Top of Mind

'Cryptocurrency' crime wave growing

by David Fitzpatrick and Drew Griffin @CNNTech

April 4, 2016, 6:14 PM ET

DHS: Ransomware attacks widely targeting feds

University of Calgary paid $20K in ransomware attack
CBC.ca - Jun 7, 2016
The University of Calgary paid a demanded $20,000 after a "ransomware" cyberattack on its computer systems. The university announced the ...

University of Calgary pays $20000 to restore email after ...
Toronto Star - Jun 8, 2016

University of Calgary pays hackers $20000 after ransomware attack
Highly Cited - Calgary Herald - Jun 7, 2016

Ransomware demands highlighted by University of Calgary
In-Depth - CTV News - Jun 8, 2016

University pays $20000 to ransomware hackers
Highly Cited - BBC News - Jun 8, 2016
The Numbers

• Cost
  – 0.5 - 5 BTC Ransom price range for decrypting files in 2016
  – $115 Price of the Amazon gift card as a alternative form of Payment
  – $17k to $20K for Notable victims

• How it spreads
  – 76% Spam
  – 16% Compromised Software, Hacking
  – 8% Compromised sites, Malvertisements and Exploit kits.

• Ransomeware Explosion
  – 50 New Variants from January to May 2016
Two Main Types of Ransomware
How it Works

Multiple Attack Vectors

Ransom Note

Trend Micro research has found over 95% of ransomware in email and web traffic

Pay Ransom
Data Decrypted – ??

OR

Data Encrypted

Restore from Backup
Ransomware History

• **History of Ransomware**
  - **Normal**
    • MAKTUBLOCKER (Artist)
    • SAMAS/SAMSAN (Server Side)
    • CERBER (Russia friendly)
    • PowerWare (Pay the Tax Person)
    • PETYA (MBR)
    • JIGSAW (Help Desk)
  - **Cool to people that do not have it.**
    • ANDROIDOS_FLOCKER (Android)
    • SYNOLOCK (Synology NAS)
    • Flocker (Smart Tv)
Fundamental Best Practices

... Necessary But Not Sufficient

Back-up and Restore
Automated: 3 copies, 2 formats, 1 air-gapped from network

Access Control
Limit access to business critical data

Keep Current with Patching
Minimize exploits of vulnerabilities

Employee Education on Phishing
Awareness, best practices, simulation testing
Throughout History Adversaries have Developed Countermeasures to Security

Prince of Wales Fort at the mouth of the Churchill River
Ransomware Disrupts Your Business

- Halts productivity and service delivery
- Loss of data on customers and core competencies that is critical to your competitiveness
- Damage to your brand and reputation
- Legal and regulatory implications
Four Layers of Protection

1. Email and Web Gateway
2. Endpoint
3. Network
4. Server
Email and Web Protection

Protection of Office 365 and Email systems before it gets to your users.

**Spear Phishing Protection**
Identify and block emails which spur users to action that will deliver ransomware

**Web Reputation**
Block access to know malicious urls

**Malware Scanning**
Scan for ransomware in emails, attachments and downloads

**Sandbox Attachments and URLs**
Detect and stop malicious URLs, document exploits, macros and scripts
Endpoint Protection

Broadest range of next-gen endpoint protection to detect and block ransomware that makes it to the endpoint.

Ransomware Behavior Monitoring
Detect and stop unauthorized encryption of multiple files

Vulnerability Shielding
Virtually patche endpoint software until it can be patched, shielding endpoints against vulnerability exploits

Application Control
Allow only know good applications to run

Lateral Movement Detection
IDS/IPS rules detect and block lateral movement of attackers

Investigation and Forensics
Discover full context, timeline and extent of attacks across endpoints
Network Protection

Detect and block ransomware from spreading on your network via unmanaged devices or other attack methods like island hopping. (Not Just Gateway)

Network Monitoring
Monitor all network ports and protocols:
- pattern and reputation analysis and script emulation
- zero-day exploits and command and control traffic

Custom Sandbox Analysis
Detect mass file modifications, encryption behavior and modifications that are consistent with ransomware
Server Protection

Server protection that stops ransomware from impacting your most critical data on your servers, whether physical, virtual or in the cloud.

- **Malware Scanning**
  Scan for malicious software and stop it

- **Vulnerability Shielding**
  Virtually patches server software until it can be patched, shielding servers against vulnerability exploits

- **Suspicious Action Monitoring**
  Detect suspicious activity on file servers related to ransomware and stops it

- **C&C Traffic Detection**
  Detect and alert on ransomware-specific command & control traffic
The Shiny Silver Bullet?

“However, history has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection.”

Trend Micro Solution

Ransomware Defense
There is no silver bullet when it comes to ransomware, but a multi-layered approach that prevents it from networks and systems is the best way to minimize the risk.

• **For Enterprises:** Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevent ransomware from reaching end users. At the endpoint level, Trend Micro Smart Protection Suites features behavior monitoring and application control, as well as vulnerability shielding to minimize the risk of getting infected by ransomware threats. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers—whether physical, virtual or in the cloud.

• **For small and medium-sized businesses,** Trend Micro Worry-Free Services Advanced offers cloud-based email gateway security through Hosted Email Security. Its endpoint protection also delivers several capabilities such as behavior monitoring and a real-time web reputation service that detects and blocks ransomware.

• **For home users,** Trend Micro Security 10 provides robust protection against ransomware by blocking malicious websites, emails, and files associated with this threat.
Visibility is Power for Early Detection and Prevention
Connected Threat Defense: Better, Faster Protection
Connected Threat Defense: Better, Faster Protection

Enable rapid response through shared threat intelligence and delivery of real-time security updates

Gain centralized visibility across the system, and analyze and assess impact of threats

Assess potential vulnerabilities and proactively protect endpoints, servers and applications

Detect advanced malware, behavior and communications invisible to standard defenses
How could you be Impacted?

• "If you don't have time to do it right, when will you have time to do it over?" - John Wooden"
Do you have an Incident Response

- Incidents will happen
- Do you have visibility
- Do make sure all teams are working together
- Do you have a Incident Manager
- Usability Vs. Security
- Do not assume
- Do not think Ransomware insurance will save you
- Multi-level security policy is now a must
- Do you know how to use the security tools on max protection
Ransomware Tomorrow?

• More focused attacks
• Part of a multi vector attacks (Go after backup first)
• Extortion model will increase
• Ransomware SAAS
• Anti Sandbox
• Home Automation
Market Leader

Gartner Magic Quadrant for Endpoint Protection Platforms

Leader for 14 straight years!
Additions to Enhance Protection

**Suspicious Action Monitoring**
Monitoring for unexpected changes to OS or installed software

**Census and Prevalence**
Uses frequency and maturity of files to determine if file is suspicious

**Ransomware Detection**
Detects and stops unauthorized encryption of multiple files

**Script & Injection Detection**
Detects scripts and/or malicious code injected into good processes

**Memory Inspection**
Unpacks files to look for fragments of known malware

**Lateral Movement Detection**
IDS/IPS rules detect and block lateral movement of attackers
Free Assessment Tool

Ransomware could hit your organization at any time, and if you’re not prepared it can be damaging. It can hurt your brand reputation, cause business disruption, and hold your valuable data hostage.

Take the Ransomware Readiness Assessment to learn tips and solutions you can use to improve your ransomware security posture.

• **Start the assessment**
Resources

Blogs
- http://blog.trendmicro.com
- http://blog.trendmicro.com/category/ransomware/

Assessment tool
Take the Ransomware Readiness Assessment to learn tips and solutions you can use to improve your ransomware security posture.
- Start the assessment

Free tools
Trend Micro

- 28 years focused on security software
- History of innovation
- 8 consecutive years on Dow Jones Sustainability Indexes
- Customers include 48 of top 50 global corporations
- 5200+ employees, 38 business units worldwide

500k commercial customers & 155M endpoints protected
Securing Your Journey to the Cloud
Thank You

PLEASE SEE US, OR EMAIL TREVOR_RICHMOND@TRENDMICRO.COM
FOR RANSOMWARE REMOVAL TOOLS
AND BEST PRACTICES
WWW.TRENDMICRO.COM
Info

- **MAKTUBLOCKER**

- **SAMAS/SAMSAN**

- **CERBER**

- **Powerware**

- **PETYA**

- **Jigsaw**

- **Flocker**
Why No One Approach is Solution

- I have listed the Pros and Cons of solutions in the market today, please take time to see in more detail why just one approach will not work
Modern Anti-Malware

- High performance
- Frees up CPU for unknown-item investigation
- Can be updated locally or from the cloud
- Accuracy can be improved with enhancements such as memory inspection and prevalence

Known Threats

- Known bad items, or those similar
- Unrecognizable threats

- Misses some unknown threats, malware evolution is rapid
- Targeted attacks can be crafted specially to avoid blacklists
- Web blacklists implemented at browser level
Application Whitelisting / Control

- Doesn’t need to identify malware
- Blocks all unknown apps
- Vendors can supply whitelist from the cloud
- Can be used for system lockdown

- Only stops EXE’s, misses other malicious items e.g. infected PDF, unless they launch an EXE
- Require configuration and management of the whitelist, with ongoing updates
- Can be vulnerable to code signing attacks

Known Good Apps

Unknown executable
Malicious non-EXE item
Behavior Monitoring / Sandboxing

- Doesn’t need to recognize specific malware
- Recognizes many suspicious behaviors (actions, log abnormality, file integrity)
- Network sandbox may prevent malware from reaching the endpoint

Item behaving suspiciously eg. ransomware

Malware evading behavior detection

- Risk of false positive
- Malware can try to detect & evade analysis
- Endpoint behavior monitoring occurs in real time, may miss early damage
- Can be more CPU intensive

Behavior Patterns
Vulnerability Shielding

• Blocks unknown threats targeting known vulnerabilities
• Helps when OS or application patches not yet available or will never be available (i.e. legacy OS)

Known Vulnerabilities

Vulnerability exploit
Malware downloads, USB items, etc.

• Can’t block malware that doesn’t exploit app / OS vulnerabilities
• Ineffective against zero-day exploits, until vulnerability rule update
Investigation / Forensics (EDR)

- Doesn’t block malware or prevent spread on its own
- Requires sophisticated IT security staff

Indicators of compromise

- Provides insight into history of malware infection
- Can help determine extent of data loss
- Can provide data to help block threat elsewhere