AGENDA

- Ransomware Overview
- Trickbot and Ryuk
- Solutions
- Q&A – Use the Q&A Panel
- Survey – It should pop up after the webinar
CDW Security Resources on this call

Presenters

Michael Lane
Sr. Field Solutions Architect
Network Security
• 2 Years at CDW
• 15 Years Industry Experience

Mikela Lea
Principal Field Solutions Architect
Information Security
• 5 Years at CDW
• 20 Years Industry Experience

Panelists

Anthony Glowacki
Inside Solutions Architect
Network Security
• 6 Years at CDW
• 10 Years Experience

Dan Siebert
Principal Field Solutions Architect
Network Security
• 4 Years at CDW
• 17 Years Industry Experience

Nathan Urbaniak
Inside Solutions Architect
Network Security
• 9 Years at CDW
• 9 Years Industry Experience
2019 RANSOMWARE IMPACT

- 118% Growth in Q1 2019
- 10 Days Average Downtime
- 96% “Customer Satisfaction”
- Average cost per security breach in education – $4,000,000

1 - 2019 Coveware Q2 Ransomware Report
2 - McAfee Labs Threats Report August 2019
3 - 2019 IBM Breach Report

$12B
Ransomware Cost in 2019

KNowBe4
“The easiest thing may be to just pay the ransom. The amount of money made by these criminals is enormous and that’s because the overwhelming majority of institutions just pay the ransom.”

Joseph Bonavolonta, Assistant Special Agent
FBI Cyber and Counterintelligence
Cyber Security Summit 2015

Paying Ransom puts your schools and others schools in further danger
Types of Ransomware

Your personal information has been stored on our servers.

Your documents, photos, databases, internernet history, emails, facebook details and more have been stored on our servers.

You only have 96 hours to submit the payment. If you do not send money within the provided time, all your data will be send to every person from your social media accounts, email address lists and other contact information found on your computer.

Press ‘View’ to view a list of all data that has been send to our servers and a list of contacts.

Press ‘Next’ for the next page

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM OR TRY TO GET THE AUTHORITIES INVOLVED. ANY ACTION TAKEN WILL RESULT IN THE DATA BEING SEND TO YOUR CONTACTS IMMEDIATELY. THE ONLY WAY TO KEEP YOUR DATA PRIVATE IS TO FOLLOW THE INSTRUCTIONS.

View  95  20  15  Next >>
How does it spread?

STOP

Your PC is infected!

Scan now

Update your antivirus (free)

:3389

:139

:445

:53
More Ransomware Characteristics

**Characteristics**
- Strong encryption
- Scrambles file names
- Delete backups
- Multiple formats and languages
- Time limit
- Infected PC is also a botnet
- Can exfiltrate data

**Evasiveness**
- Polymorphic
- Staying dormant
- Sophisticated encryption of Command & Control (C2) traffic and payload
- Anonymity via TOR and BTC
- Fast Flux: rapid DNS to IP mappings
- Domain shadowing: creating subdomains with stolen cred’s to avoid reputation-based filters
- Use Domain Generation Algorithms to dynamically generate domains for Command C2 traffic
Silent Threat: Crypto-Mining Software

New Coin Miner Malware

Trickbot & Ryuk
TRICKBOT

Unpaid Invoice

Our records indicate that payment on your account is overdue in the amount of $23,508.41. If
the amount has already been paid, please disregard this notice. For your convenience, a copy of
your invoice has been attached below, please save it for future reference.

If you have any query regarding your account or disagree that this invoice is overdue, please
email accounts@intuit.com. Note that if we do not hear from you or receive the payment in the
nearest future, your account will be suspended.

Sincerely,

Accounting Department
Gary Terry
Level 3 Officer, Intuit
Email: Gary.Terry@Intuit.com

MS17-010

Trickbot C2 Servers

Ryuk Package
RYUK

Gentlemen!

Your business is at serious risk. There is a significant hole in the security system of your company. We’ve easily penetrated your network.

You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks. They can damage all your important data just for fun.

Now your files are encrypted with the strongest military algorithms RSA-2048 and AES-256. No one can help you to restore files without our special decoder.

Photos, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.

If you want to restore your files, write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files (less than 5 Mb each, non-archived and your files should not contain valuable information (databases, backups, large excel sheets, etc.)). You will receive decrypted samples and our conditions how to get the decoder.

Please don’t forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins. The final price depends on how fast you write to us. Every day of delay will cost you additional +0.5 BTC.

Nothing personal just business.

As soon as we get bitcoins you’ll get all your decrypted data back. Moreover you will get instructions how to close the hole in security and how to avoid such problems in the future. + we will recommend you special software that makes the most problems to hackers.

Attention! One more time!

Do not rename encrypted files. Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers. We don’t need your files and your information. But after 2 weeks all your files and keys will be deleted automatically. Just send a request immediately after infection. All data will be restored absolutely. Your warranty – decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLwDvnm5in7mTvU12jg67wt86dhqUyNj

Ryuk

NO system is safe
What can you do?

Network Access Control
Next Generation Firewalls
Security Incident and Event Management
Security Orchestration, Automation, and Reporting
Next Generation Endpoint Protection
URL Filtering  DNS Filtering  Mobile Device Management
Data Loss Prevention
Cloud Access Security Broker
Advanced Phishing Protection
Role Based Access Control
Assess your current security and risks
Software Patching

- Working on updates
  - 20% complete
  - Don’t turn off your computer
Passwords and Trust Relationships

D*c90>+2

G0BlackHawks!

crow win scienc3 house
Internal Penetration and Pivoting

- Initial Workstation
- Elevate Privileges
- Access Servers & Resources

Initial Workstation → Elevate Privileges → Access Servers & Resources
Mikela’s Hierarchy of Logging

**Tier 0**
Poorly Configured, Rolls over regularly, possibly not logging at all

**Tier 1**
Useful Information, but too much of it!

**Tier 2**
Tools like Splunk or Sawmill – doesn’t correlate, takes time

**Tier 3**
Correlates but expensive / high maintenance

**Tier 4**
Best!

**Trained Human**
SIEM / SOAR
HTML Reporting and log review
Off-device logging
Default logging

Best!
Phishing
Phishing – How I do it

• **TIP:** Using a different format for user ID’s and e-mail addresses makes it harder for attackers, as it’s much harder to find the login ID than the e-mail address

• Focus on: Teachers, Office Staff, Finance

• Avoid: IT

• Create customized phishing emails:
  • “bypass your organization’s firewall and content filter”
  • General messages from I.T. – new requirements, testing
  • Amazon gift card for participating in a survey
  • Infected PDF documents – tracking from UPS or a vendor invoice that looks just legit enough to open
  • Amazon Prime Day is the biggest phishing day of the year
Training and Testing

This email is clearly not from Facebook.

The “Go To Facebook” link goes to “icpnet.pl”, not Facebook.

No indication that they know who you are.

No name or other contact details, although automated messages are less likely to have that information.
TRICKBOT & RYUK

Stop it here with Email Security & Phishing Protection

Stop it here with Next Gen endpoint protection

Stop it from spreading with patch discipline

Stop it here with strong Next Gen Firewalls and DNS level filtering

Recover from an event with solid backups

Stop it from spreading with network segmentation

Recover from an event with solid backups

Ryuk Package

Trickbot C2 Servers
Our Top 5 Recommendations
OUR TOP 5 RECOMMENDATIONS

#1: Implement Next Generation Endpoint Protection

SOPHOS
CISCO
CROWDSTRIKE
TREND MICRO
Carbon Black.

paloalto
together is power.

McAfee

Together is power.
#2: Implement DNS Filtering

91% of C2 can be blocked at the DNS layer

15% of C2 bypasses 80 & 443
#3: Conduct a Security Assessment

OUR TOP 5 RECOMMENDATIONS

- Rapid Security Assessments
- Comprehensive Security Assessments
- Application Security Assessments
- Policy development
- Framework / Controls Gap Analysis
- Table Top for Incident Response
#4: Educate your users

- 77% of threats require user intervention
- Conduct regular phishing exercises
- Provide end users with phishing education
#5: Implement Strong Patch and Backup Discipline
ZERO-COST CDW THREAT CHECK

WHAT'S LURKING ON YOUR NETWORK

Carbon Black.

CDW Threat Check goes beyond malware identification, providing guidance for threat remediation and a whole lot more:

Easy, guided deployment

Practical

Non-intrusive

Schedule your zero-cost CDW Threat Check!
TOP CTC RESULTS

Top Five Technical Findings
1. Active Crypto mining
2. Cleartext Credentials Captured
3. Anonymous Browsing VPNs (UltraSurf, CyberGhost, etc.)
4. Use of Unsanctioned Cloud Storage
5. Active Known Malware

Top Five Common Weaknesses
1. Insufficient malware protections (Network or Endpoint)
2. Weak Password Controls
3. Insufficient Logging/Monitoring
4. No Incident Response Plan
5. Insufficient Network Segmentation
ZERO-COST INCIDENT RESPONSE RETAINER

• Have a security breach?

• Assistance with
  • Incident Triage
  • Containment
  • Remediation
  • Response Report

• No cost up front

• Sleep better at night
TOP 5 RECOMMENDATIONS RECAP

#1: Implement Next Generation Endpoint Protection

#2: Implement DNS Filtering

#3: Conduct a Security Assessment

#4: Educate your users

#5: Implement Strong Patch and Backup Discipline
STAY PARANOID AND TRUST NO ONE