ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Ryuk: Protecting Clinical Engineering from Ransomware Attack

Dr. Saif Abed, MD

The AbedGraham Group
Clinically Optimized Success

Tracey Hughes

DukeHealth

Pablo Rincon Crespo

CYLERA LABS

Richard Staynings

CYLERA

December 02, 2020

Session Description

Please join healthcare thought leaders, including Clinical Engineering executives, Cyber Security specialists, CMOs, CISO's and MDs for a diverse, thoughtful and deeply interesting panel discussion on preparedness for Ryuk, its impact on the healthcare industry.

About the moderator

Richard Staynings, Chief Security Strategist, Cylera

Richard Staynings is a globally renowned thought leader, author, public speaker and advocate for improved cybersecurity across the Healthcare and Life Sciences industry.

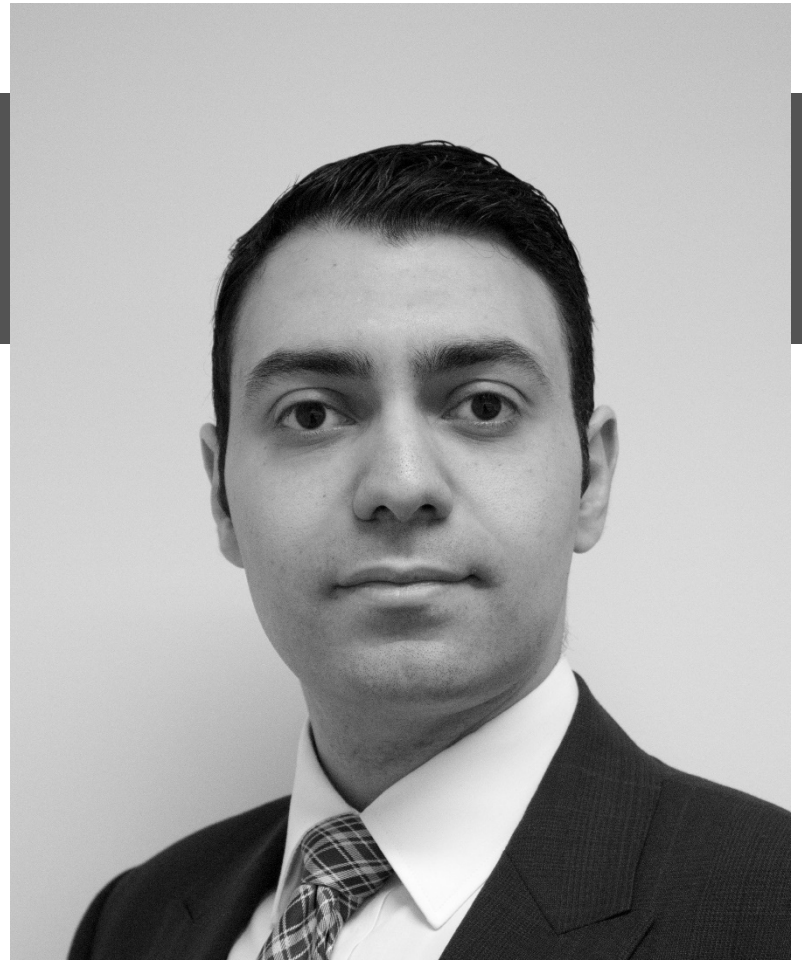
He has served on the global HIMSS Privacy and Cybersecurity Committee and on the board of CHIME / AEHIS. Richard has advised numerous government and industry leaders on their healthcare security strategy and defensive posture, as well as serving as a subject matter expert on government Committees of Inquiry into some of the highest profile healthcare breaches.

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the “Q&A” feature in Zoom at any time.
- If there is any urgent issue, please use the “chat” feature to communicate with the panelists.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the speaker

The AbedGraham Group
Clinically Optimized Success



Dr. Saif Abed, MD

Dr. Abed is a medical doctor and healthcare cybersecurity/national security expert. His primary fields of specialisation are cyber-warfare and crime targeting hospitals and safety critical infrastructure.

Based in London, Dr Abed is a Partner and Director of Cybersecurity Services at the clinical security advisory and technology firm, The AbedGraham Group, and holds additional independent expert roles for the European Commission, World Health Organisation and UK Infrastructure and Projects Authority.

Academically, he holds degrees in Medicine (St.George's Hospital Medical School, University of London), Management (Cambridge University) and Software and Systems Security (Oxford University).

About the speaker

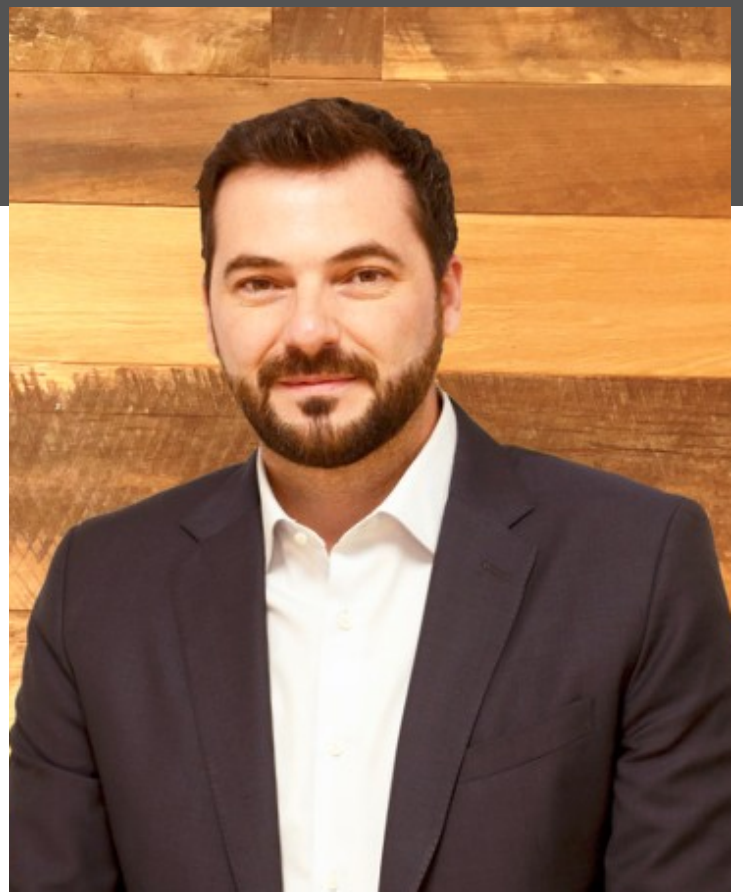
Tracey Hughes is the Senior Director of the Clinical Engineering at Duke Health Technology Solutions. Her leadership, clinical engineering and healthcare technology expertise spans more than thirty years. She spent the first twenty years of her career with Aramark Healthcare (now TRIMEDX) having achieved the position of Vice President of Operations for Clinical Technology Services.

Her current responsibilities with Duke Health include oversight of the clinical engineering management program – with oversight of over 55,000 active medical devices – as well as working closely with the ISO, Compliance and Supply Chain on cybersecurity surrounding medical devices. Tracey has earned a Bachelor's of Science in Biomedical Engineering Degree from Tulane University and a Master's of Management in Clinical Informatics Degree from Duke University School of Medicine.

Tracey Hughes

About the speaker

CYLERA LABS

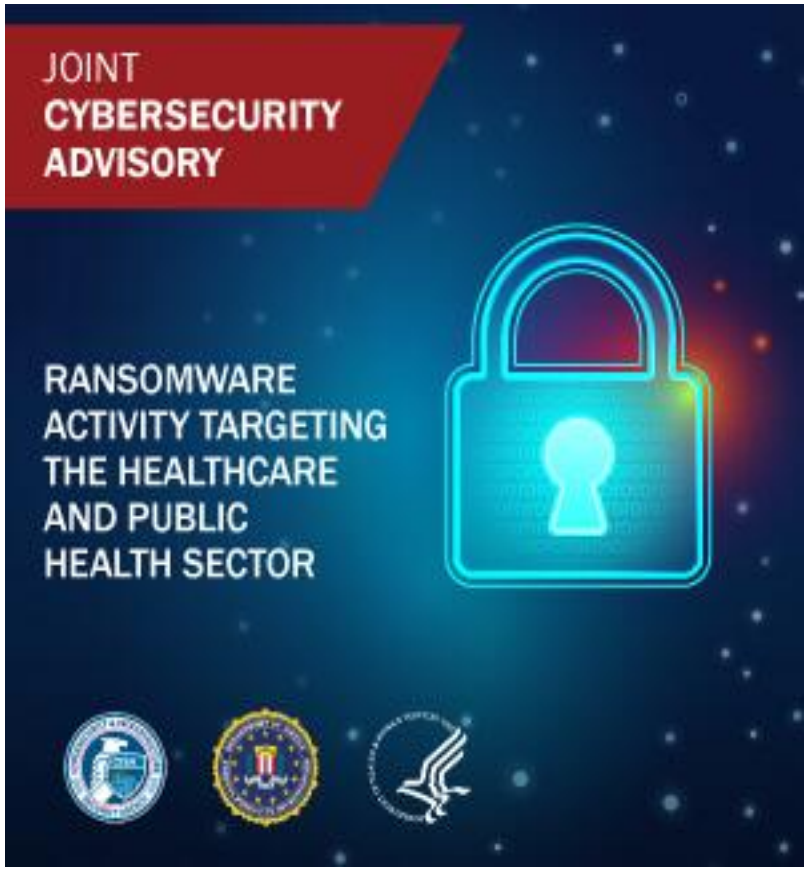


Pablo Rincon Crespo

Based in Madrid, Pablo Rincon is VP of Cybersecurity at CyleraLabs, specializing in medical device protection and vulnerability management. He is an authority in the space of cyber threat intelligence, highly specialized in Healthcare APTs like Orangeworm, being first to spot the relation of Kwampirs with Shamoon APT and has presented some of his findings at security conferences all over the world.

Before joining the Cylera team, Pablo worked for companies such as AlienVault, Emerging Threats, Qualys, Buguroo, his own startup and Suricata (OISF), and has participated in the design and development of a wide range of security solutions, SIEM, IPS, WAF, Digital Surveillance and Early Warning Systems, Vulnerability Management, and Information Leak Prevention Systems. He has also collaborated in Incident Response, forensics and malware analysis for IBEX35 companies.

Ryuk


JOINT
CYBERSECURITY
ADVISORY
RANSOMWARE
ACTIVITY TARGETING
THE HEALTHCARE
AND PUBLIC
HEALTH SECTOR


RYUK
Ransomware

First, some background on Ryuk

What is Ryuk, where did it come from and who is using it?

- Ransomware, cyber extortion, evolution of cybercrime strategy
- Ransomware predominance for the last 3 ~ 5yr
- Ryuk precursor *Hermes* developed by *CryptoTech*:
- - *Hermes*, RaaS (Ransomware as a Service), $300
- - *Hermes* 2.1 → *Ryuk*
- - As of today attribution still unclear
- Cyber criminals use it for profit. Many researchers believe the Ryuk actors have ties with "*Trickbot*" banking malware (FireEye *UNC1878*, CrowStrike *Wizard Spider*)

What is Ryuk, where did it come from and who is using it?

hermes 2.1 ransomware

By CryptoTech, August 22, 2017 in [Software] - malware, exploits, bundles, crypts

1 2 3 4 NEXT » Page 1 of 4

CryptoTech

kilobyte

User

5

40 posts

Joined

11/29/16 (ID: 74394)

Activity

другое

Posted August 22, 2017 (edited)

Hermes 2.1 Ransomware

*Software does not work in RU,UA,BY countries.

*work offline, communication by e-mail.

*Write on C

*Build size 45-55kb.

*Work on x86/x64, servers: 2003 and higher,XP,7,8,10.

*Encryption method AES256 + RSA2048, unique key for each pc, and each file.

*Only RSA private key holder can decrypt files, malware reseacher's confirm it

How does it work? What is the Ryuk Attack Kill Chain?

1)Simplifying the stages:

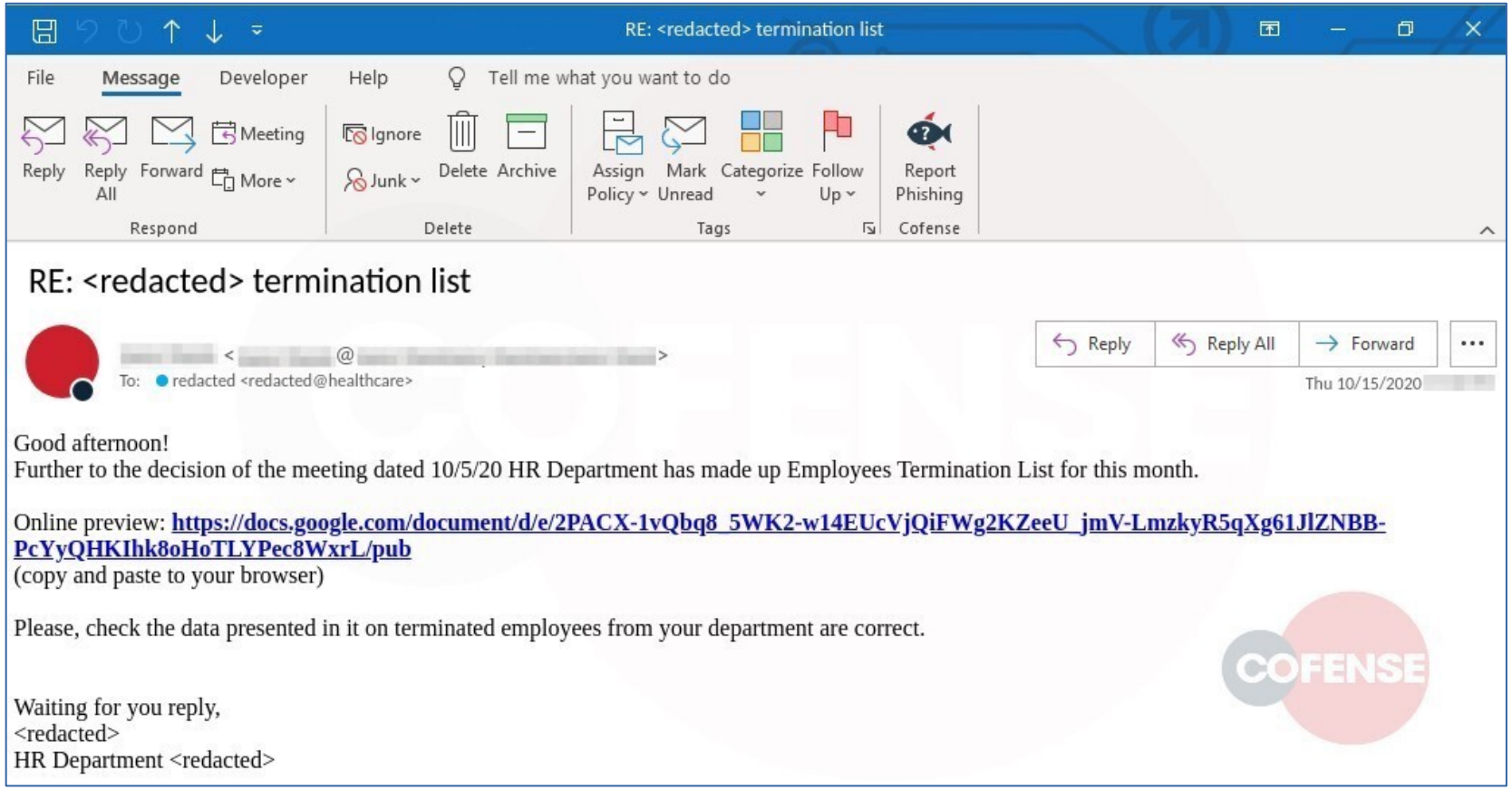
2) Initial infection vector

3) Reconnaisance stage and lateral movement

4) Ryuk delivery and execution

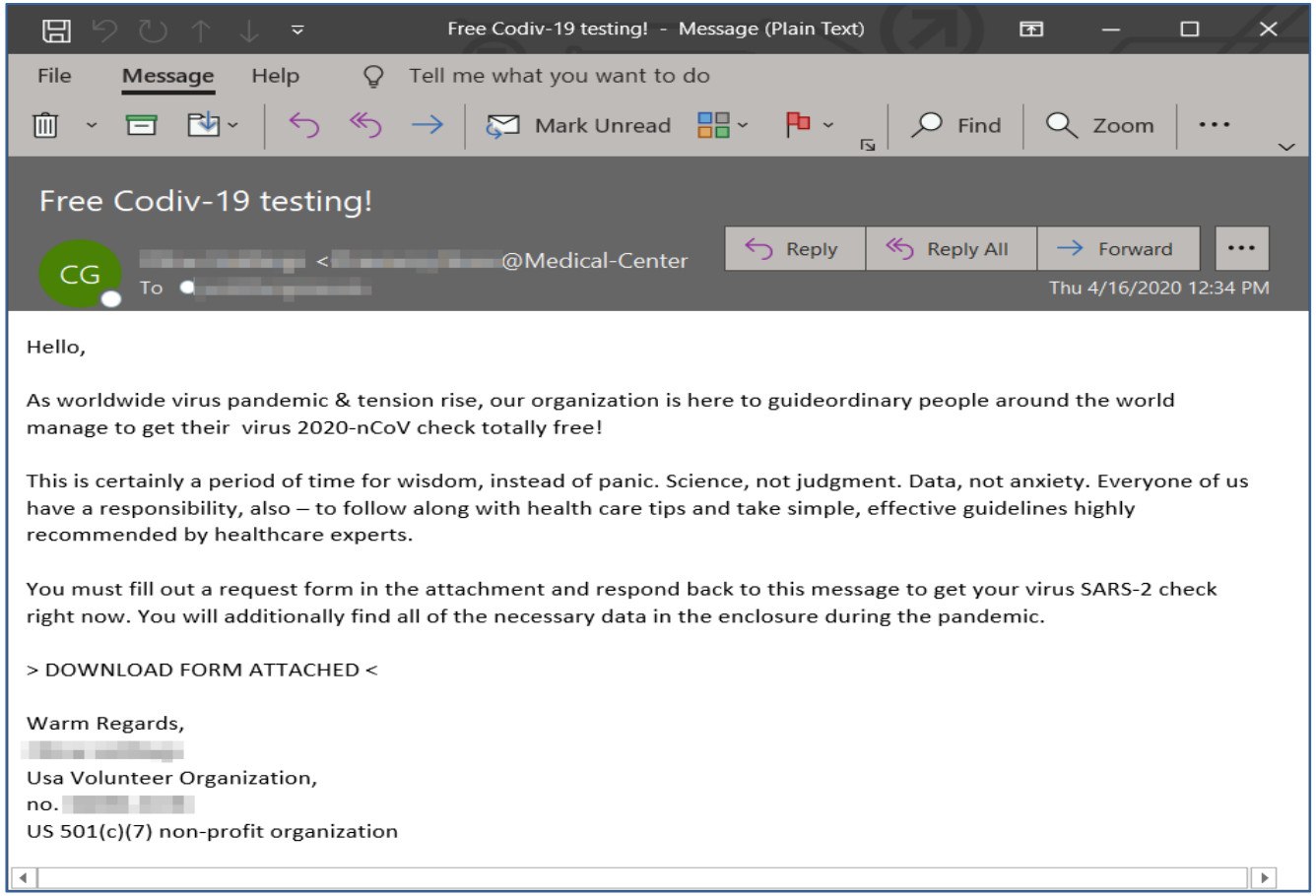
Usual chain: Lure doc → *Emotet* → *Trickbot* (+ *Cobalt Strike*)→ *Ryuk*

1. Initial infection vector



Source: COFENSE

1. Initial infection vector



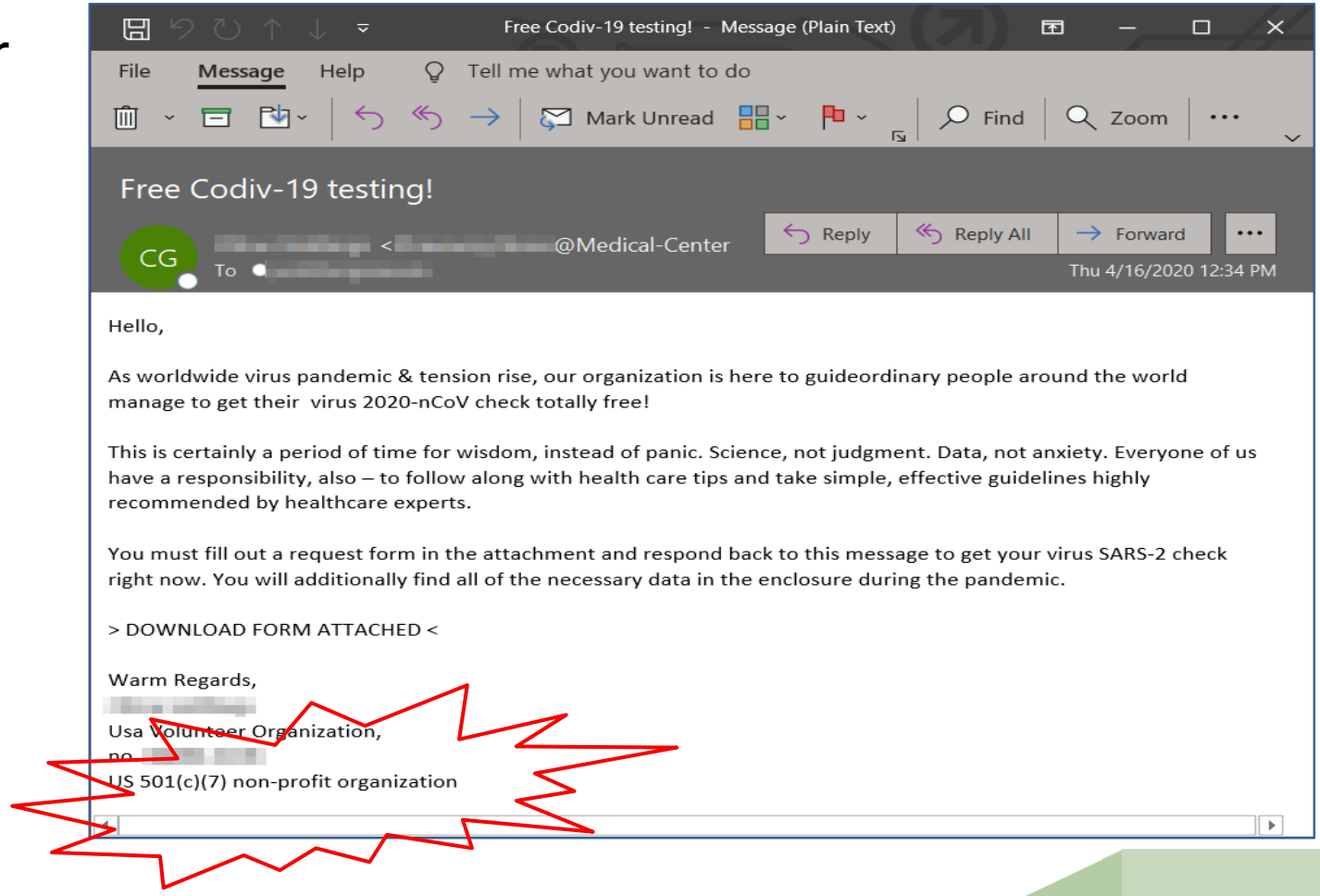
Source: EDSI Trend

1. Initial infection vector

- Lure documents on malicious emails (“spear phishing” campaigns)
  - Usually drop *Emotet*, *BazarLoader* via PS scripts (then *Trickbot*)
  - Sometimes they use *Zloader (Zbot*)
- Devices and services exposed to internet
  - Vulnerable devices, servers and workstations (ie: *Bluekeep*, *Zerologon*)
  - Default or easy to “bruteforce” credentials on services: SSH, telnet, RDP, FTP
- Credentials of victims are “goods” sold in underground forums
- - One user and password sold for thousands of dollars can have a ROI

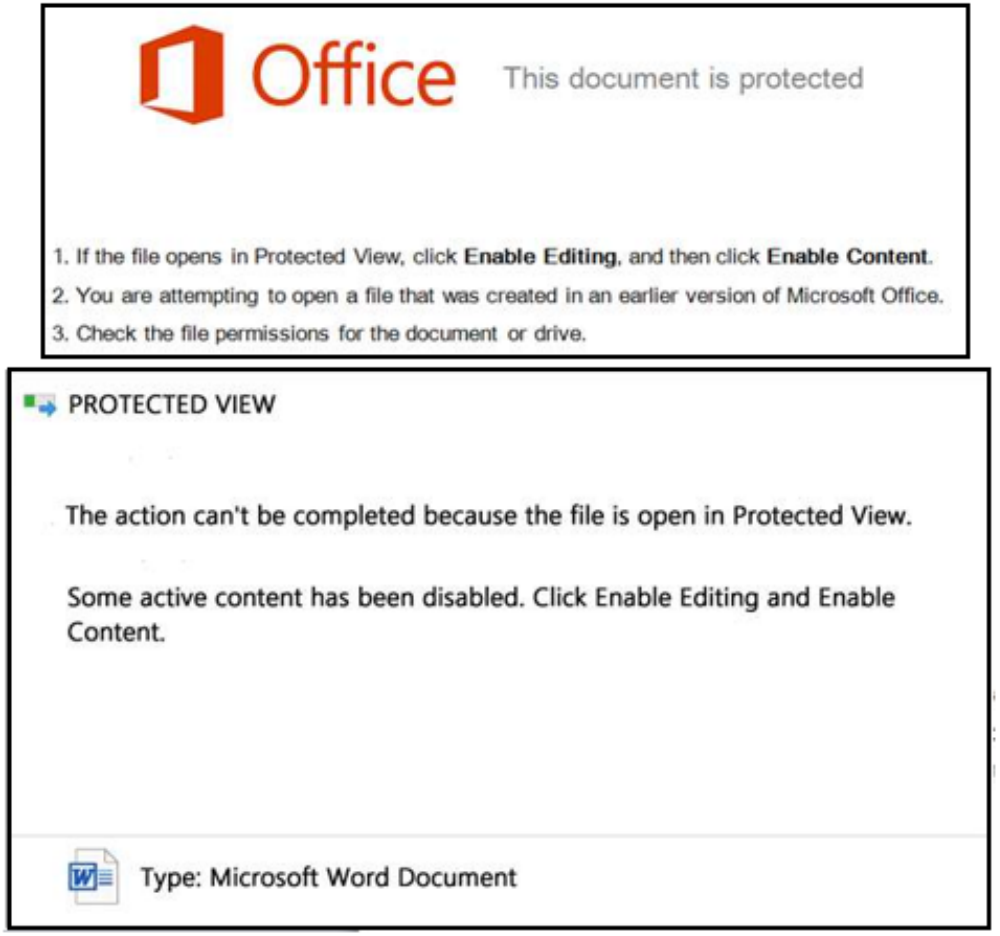
Ryuk Threat Briefing slides

1. Initial infection vector



Source: EDSI Trend

1. Initial infection vector



Source: EDSI Trend

2. Reconnaisance stage and lateral movement

- Find AD Domain Controllers, primary but also secondary
- Gather domain credentials, also pivot on available domains
- Identify valuable targets (depends on industry), often exfiltrating data:
  - In healthcare can be EMR, PACS servers
  - Point of Sales, devices used for filling forms
  - Databases
  - Grab user browser credentials

2. Reconnaisance stage and lateral movement

- Some of the tools used for this:
  - *Trickbot* w/ modules, *Cobalt Strike*
  - *Mimikatz*, *SharpHound*, *Rubeous*, *ADFind*
  - WMI, PowerShell, *psexec*, icacls, *Putty*, RDP, FTP
- Periodically they tend to innovate/refresh/switch the tools used

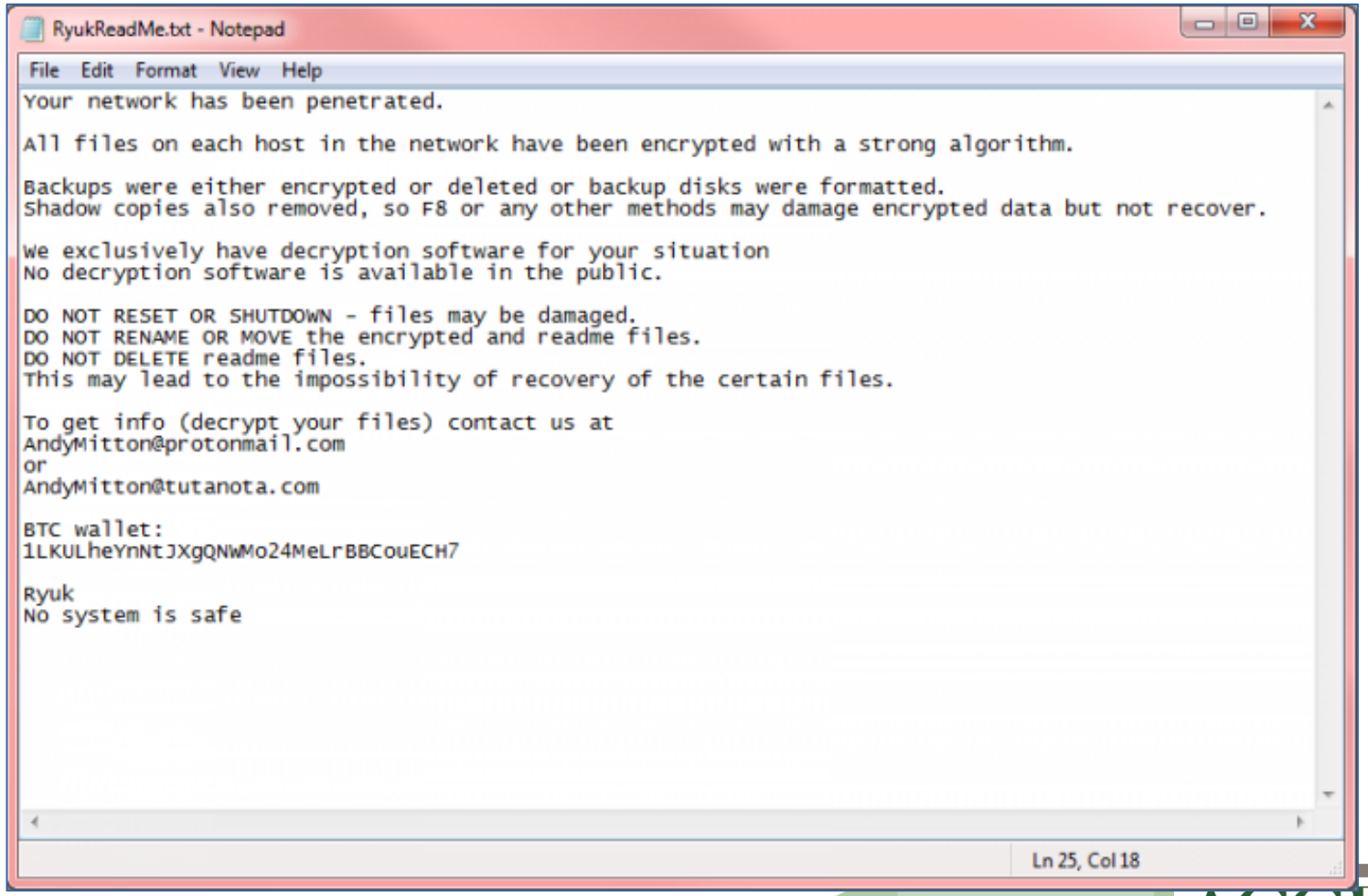
3. Ryuk delivery and execution

- Distributing Ryuk is also often done via RDP (clipboard transfer), windows shared folders, PowerShell, sheduled jobs, windows GPOs
- Bakckups will be removed (also they will try to disable antiviruses, and shadow copies)
- Ryuk will:
  - Send wake on land packets for stand-by devices/workstations
  - Send ping requests to identify possible victim hosts and will try to mount unit drives
- Launch multiple execution threats to encrypt files at local and remote drives (even created by them)

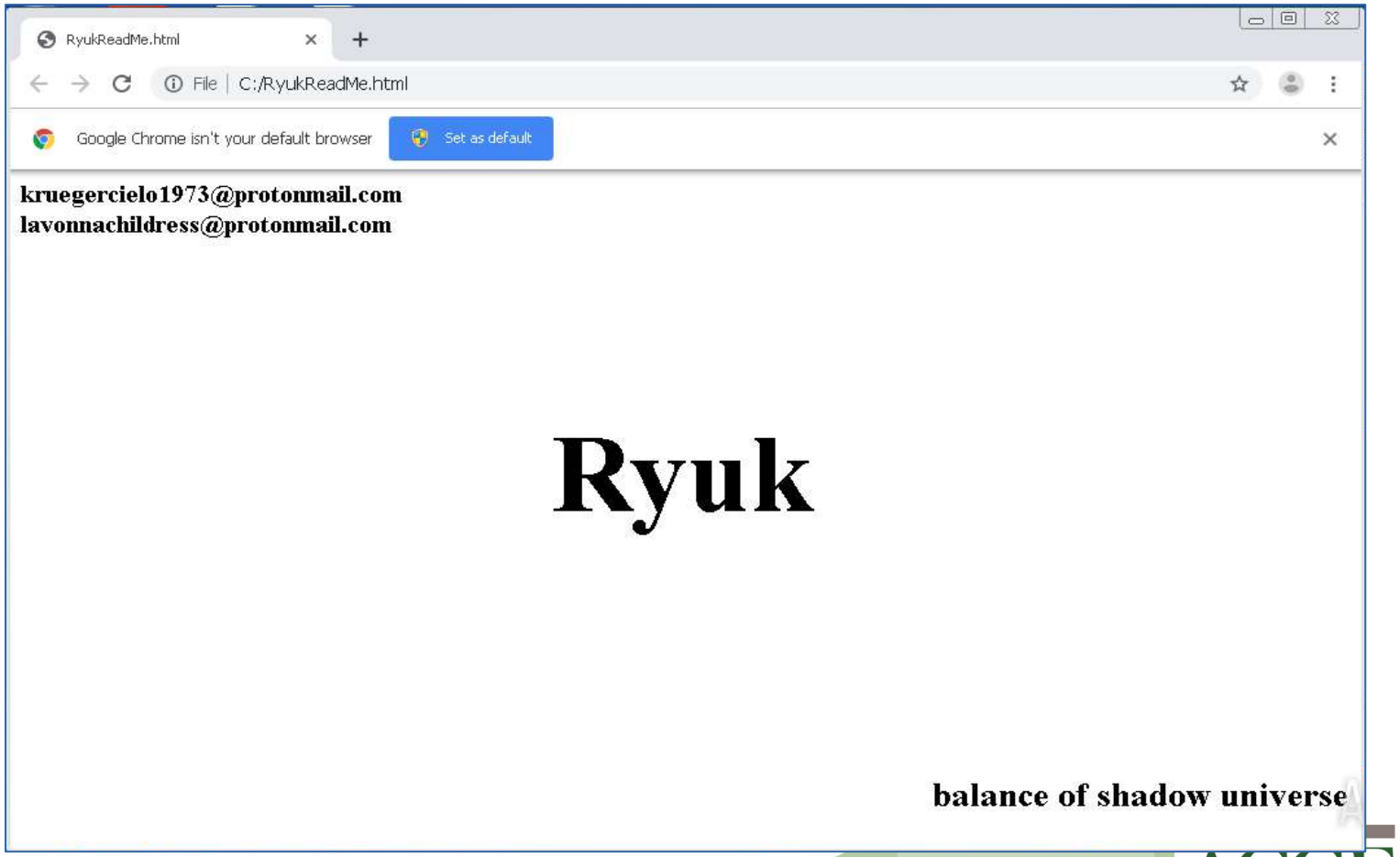
3. Ryuk delivery and execution

- Each thread will generate and use an AES256 encryption key. This keys will be encrypted with an RSA key that’s embbeded at the ryuk resources
- After encryption, files will be renamed to have the extension .ryk
- A note will be added in the encrypted directories
- It will be displayed, with an email address, an ammount and a bitcoin address

3. Ryuk delivery and execution



3. Ryuk delivery and execution



Panel Discussion

Why is ransomware like Ryuk so dangerous to healthcare?

- A clinician’s perspective
- A clinical engineer’s perspective

How do you know when you have been hit with Ryuk?

What are the IoCs?

- Up-to-date IOCs → feed subscriptions; constantly review new reports; Review US-CERT IOCs*
- At host level, files with ".ryk" extension means the host is already compromised
- Network level:
  - Look for http requests to external IPs (without domain name), or with cheap TLD domains (.bazar, .xyz, .jo,), random strings (nutqauytva513xyzf11zzzzz0[.]com) (see the examples)
  - Out of hours connections, anomalous traffic.. (for this you need to get used to your traffic profile)
  - Look for anomalous RDP, telnet, ssh connections, not only external, also internal.
  - Review scheduled jobs and GPOs

- *(*) US-CERT IOCs: https://us-cert.cisa.gov/ncas/alerts/aa20-302a)*

How do you know when you have been hit with Ryuk? What are the IoCs?

- Emotet URLs:
- - hxxps://fysinstitute[.]com/hoaw62idks/xj/
- - hxxps://my-way[.]style/8mjle980/vdCYhx/
- Trickbot:
  - hxxp://199.38.121[.]150/mor137/WALKER-PC_W617601.E4BBAE191487762D596C33B195D5C2BB/5
  - hxxps://185.99.2[.]66/ono48/WALKER-PC_W617601.2FFAA681BE244D35AE66D42BF113F6D5/5/spk
- Any url ending in scripts named or containing the word “gate”, like “gate.php”, “gateJ5bnh4gr.php”, or “cp.php” should trigger a review
- Wake-on-land packets or unusal icmp/ping traffic (scanning)

How do you know when you have been hit with Ryuk? What are the IoCs?

“What is my ip” queries:

- ipecho[.]net
- api[.]ipify[.]org
- checkip[.]amazonaws[.]com
- ip[.]anysrc[.]net
- wtfismyip[.]com
- ipinfo[.]io
- icanhazip[.]com
- myexternalip[.]com
- ident[.]me

‘Being Prepared’ is more that a Boy Scout motto. What should clinical engineers and others do today?

- Accurate, real-time inventory that includes IT attributes such as IP, MAC, OS, patching, endpoint security, etc.
- Work with Procurement to include language regarding SBoM, patching in purchases
- Evaluate passive discovery tools available to assist with overall visibility and transparency of medical devices (inventory, risk management and prioritization of work effort). Do a proof of concept (or several) and build a business case to support implementation of one of these solutions
- Identify areas that if compromised would have greatest impact to patient safety and hospital operations

‘Being Prepared’ is more that a Boy Scout motto. What should clinical engineers and others do today?

- Now, more than ever, work with your IT teams
- Profiling of medical devices
- Recommentations for policy regarding communication between devices
- Understanding vulnerabilities that impact medical devices with focus on critical vulnerabilities
- Segmentation
- Visibility within the IT CMDB (configuration management database)

‘Being Prepared’ is more that a Boy Scout motto. What should clinical engineers and others do today?

- Now, more than ever, work with your manufacturers
- Bookmark your manufacturer’s security websites-. Most of the larger manufacturers today have dedicated sites that assist with identification of threats within their product base and latest patching information
- Build strong relationships with your local support teams
- Remind manufacturers that remote access may need to be turned off or limited during high threat situations
- If you maintain service contracts ensure they include language about patching and remaining current on OS levels

‘Being Prepared’ is more that a Boy Scout motto. What should clinical engineers and others do today?

- Work to make your organization aware of equipment that is not traditionally included in medical equipment inventories (examples we have found include Pyxis and Omnicell work stations) and may represent a gap in management and oversight.
- Work with clinical leadership on response, containment and recovery if a medical device is impacted or a threat is detected
- Awareness of resources that are available
  - https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf
  - https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- Share with the HTM community

How should we coordinate with clinical leaders (e.g. CMIOs) to improve security posture?

What can / should you do to prevent a Ryuk attack?

Patching, NAC, Quarantine, but first understand your risks

Beyond well-known metrics like CVSS how do we qualify and quantify patient safety and clinical service risks?

The importance of leadership

Final Survival Tips

- Event monitoring, SOC/MSSP SIEM, use IOC feeds:
  - Network traffic monitoring, specially devices you can’t install things on
  - AD & host event monitoring
- Use microsegmentation, NAC, firewalling
- Know what you expose to internet, why, and ensure a good patch/updates level
- Avoid at all cost using default passwords, or master passwords
- EDR and Antivirus solutions
- Offline backups (b/c are also their most valuable targets)
- Periodical audits: blue team, red team, purple team exercises. Adversary emulation

Final Survival Tips

- They run a lot, you should too (months → days → hours → 2 hour attacks)
- Prepare a contingency plan for proactive resilience:
  - selective quarentine, what can be powered off, what can be unplugged, what can't, also know what shouldn't be affected.
  - Find a balance for the short-mid term (what happens next days)
- Prepare the recovery process for an incident
  - It's not just power on and run a vaccum/av. How to backup recovery.
  - Iterative, ordered, hands-on process backed with monitoring
  - What's critical for patient safety and business continuity
- Who will lead this plans. Assign responsibilities. Communication (inside, outside)

Final Survival Tips

- Train your team. Protect from social engineering attacks
- Don’t use your personal email at work
- Be careful with BYOD
- Don’t open emails with attachments, or links, when you don’t know who is the sender. Validate and verify through other communication channels
- For common workstations, and many of the systems, a common recommendation is to power them off as soon as possible (try limit the damage).

Audience Questions

Thank You

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING