LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

APT and Cybercriminal Targeting of HCS

June 9, 2020

Agenda

- Executive Summary
- APT Group Objectives
- APT Groups Targeting Health Sector
- Activity Timeline
- TTPs
- Malware
- Vulnerabilities
- Recommendations and Mitigations

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Executive Summary

- APT groups steal data, disrupt operations, and destroy infrastructure. Unlike most cybercriminals, APT attackers pursue their objectives over longer periods of time. They adapt to cyber defenses and frequently retarget the same victim.
- Common HPH targets include:
  - Healthcare
  - Biotechnology
  - Medical devices
  - Pharmaceuticals
  - Healthcare information technology
  - Scientific research
- HPH organizations who have been victim of APT attacks have suffered:
  - Reputational harm
  - Disruption to operations
  - Financial losses
  - PII/PHI and proprietary data theft
- HC3 recommends several mitigations and controls to counter APT threats.

APT Group Objectives

- Motivations of APT Groups which target the health sector include:
- Competitive advantage
  - Theft of proprietary data/intellectual capital such as technology, manufacturing processes, partnership agreements, business plans, pricing documents, test results, scientific research, communications, and contact lists to unfairly advance economically.
- Intelligence gathering
  - Groups target individuals and connected associates to further social engineering or other attacks.
- Financial gain
  - Information stolen or held for ransom are used to gain financially; victims include both health sector organizations and patients.

Image: Creative Commons

APT Groups Targeting Health Sector

Group	Active Since	Also Known As/Associated Groups	Targets	Description
FIN4(1)	2013		Healthcare Pharmaceutical	• Unique in that they do not infect victims with characteristic malware, instead capture email credentials
Orangeworm(2)(3)	2015		Healthcare Healthcare IT Medical Devices Pharmaceuticals	• Corporate espionage
Deep Panda(4)	2011	Shell Crew WebMasters KungFu Kittens PinkPanther Black Vine	Healthcare Pharmaceuticals	• Chinese; responsible for Anthem breach
APT10(5)	2009	menuPass Stone Panda Red Apollo CVNX Cloud Hopper HOGFISH	Healthcare Medical Devices Pharmaceuticals Biotechnology	• Chinese cyber espionage group

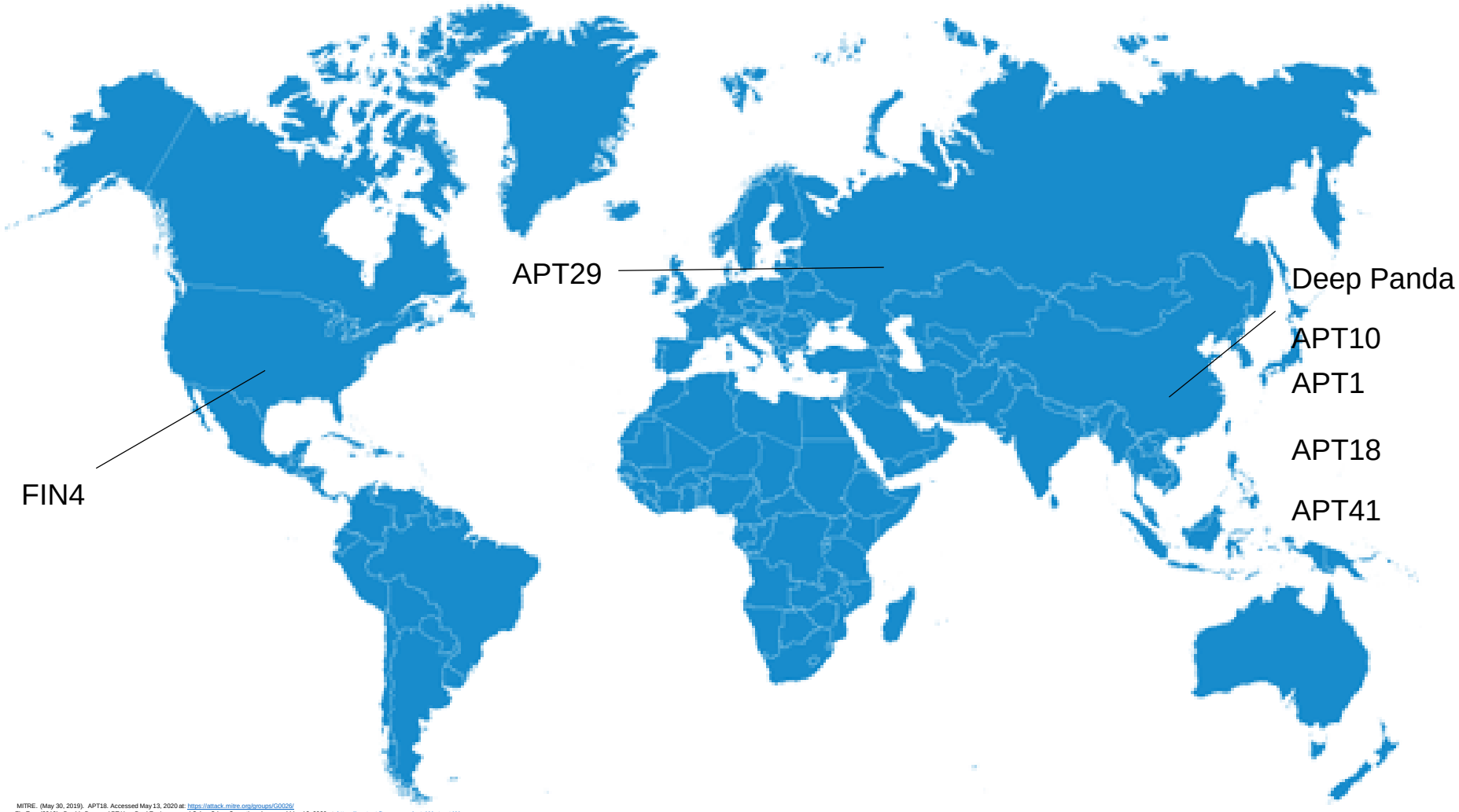
1 MITRE. (April 18, 2019). FIN4. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0085/
2 Symantec. (April 23, 2018). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Accessed May 13, 2020 at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
3 MITRE. (March 25, 2019). Orangeworm. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0071/
4 MITRE. (October 11, 2019). Deep Panda. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0009/
5 FireEye iSight Intelligence. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. FireEye. Accessed May 13, 2020 at: https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

APT Groups Targeting Health Sector

Group	Active Since	Also Known As/Associated Groups	Targets	Description
APT18[1]	2009	TG-0416 Dynamite Panda Threat Group-0416 Wekby	Healthcare Biotechnology	• Suspected Chinese APT group • Frequently developed or adapted zero-day exploits for operations, which were likely planned in advance.
APT41[2]	2012		Healthcare Medical Devices Pharmaceuticals Biotechnology	• Chinese state-sponsored espionage and financially motivated activity
APT22[3]			Healthcare Biomedical Pharmaceutical	• Multi-year targeting of health center focused on cancer research
APT1[4]	2006	Unit 61398 Comment Crew Comment Group Comment Panda	Scientific Research and Consulting Healthcare	• Chinese cyber espionage group
APT29[5]	2008		Pharmaceutical Healthcare Biotechnology Scientific Research and Consulting	• Russian cyber espionage group

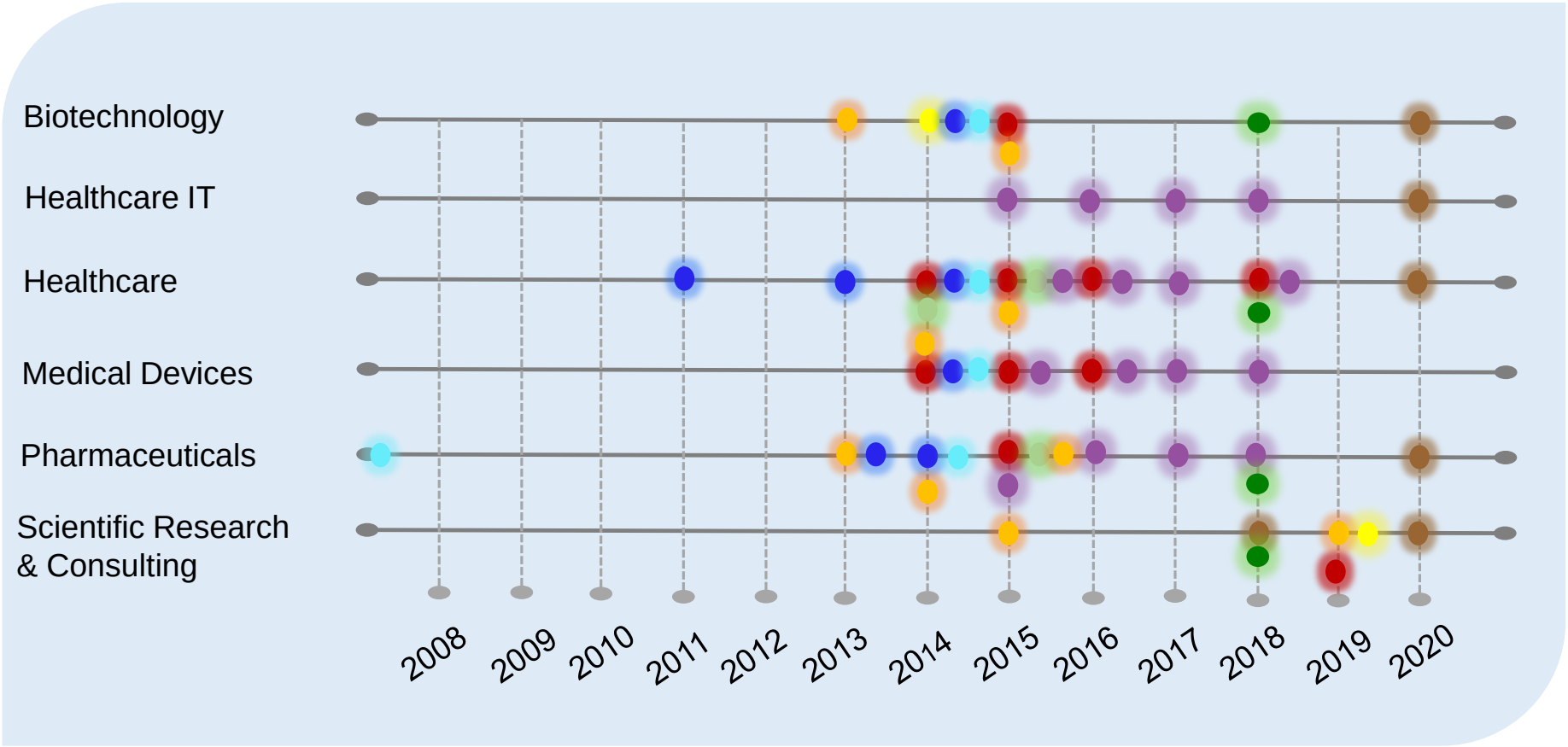
1 MITRE. (May 30, 2019). APT18. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0026/
2 FireEye. (2019). Double Dragon APT41, a Dual Espionage and Cyber Crime Operation. Accessed May 13, 2020 at: https://content.fireeye.com/apt-41/rpt-apt41/
3 Osborne, C. (August 21, 2019). Cancer Research Organizations Are Now The Focus of Chinese Hacking Groups. ZDNet. Accessed May 13, 2020 at: https://www.zdnet.com/article/cancer-research-organizations-become-the-new-focus-of-chinese-hacking-groups/
4 Mandiant. (n.d.) APT1 Exposing One of China's Cyber Espionage Units. Accessed May 13, 2020 at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
5 MITRE. (July 25, 2019). APT29. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0016/

APT Groups Targeting Health Sector



MITRE. (May 30, 2019). APT18. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0026/
FireEye. (2019). Double Dragon APT41, a Dual Espionage and Cyber Crime Operation. Accessed May 13, 2020 at: https://content.fireeye.com/apt-41/rpt-apt41/
Osborne, C. (August 21, 2019). Cancer Research Organizations Are Now The Focus of Chinese Hacking Groups. ZDNet. Accessed May 13, 2020 at: https://www.zdnet.com/article/cancer-research-organizations-become-the-new-focus-of-chinese-hacking-groups/
Mandiant. (n.d.) APT1 Exposing One of China's Cyber Espionage Units. Accessed May 13, 2020 at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
MITRE. (July 25, 2019). APT29. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0016/
MITRE. (April 18, 2019). FIN4. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0085/
Symantec. (April 23, 2018). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Accessed May 13, 2020 at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
MITRE. (March 25, 2019). Orangeworm. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0071/
MITRE. (October 11, 2019). Deep Panda. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0009/
FireEye iSight Intelligence. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. FireEye. Accessed May 13, 2020 at: https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

APT Groups Targeting Health Sector Activity Timeline



APT41 APT22 DEEP PANDA APT10 APT18 APT29 FIN4 APT1 ORANGEWORM UNSPECIFIED

MITRE. (May 30, 2019). APT18. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0026/
FireEye. (2019). Double Dragon APT41, a Dual Espionage and Cyber Crime Operation. Accessed May 13, 2020 at: https://content.fireeye.com/apt-41/rpt-apt41/
Osborne, C. (August 21, 2019). Cancer Research Organizations Are Now The Focus of Chinese Hacking Groups. ZDNet. Accessed May 13, 2020 at: https://www.zdnet.com/article/cancer-research-organizations-become-the-new-focus-of-chinese-hacking-groups/
Mandiant. (n.d.) APT1 Exposing One of China's Cyber Espionage Units. Accessed May 13, 2020 at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
MITRE. (July 25, 2019). APT29. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0016/
MITRE. (April 18, 2019). FIN4. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0085/
Symantec. (April 23, 2018). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Accessed May 13, 2020 at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
MITRE. (March 25, 2019). Orangeworm. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0071/
MITRE. (October 11, 2019). Deep Panda. Accessed May 13, 2020 at: https://attack.mitre.org/groups/G0009/
FireEye iSight Intelligence. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. FireEye. Accessed May 13, 2020 at: https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

TTPs

Password Spraying[1]

- **Scanning** external websites of targets looking for vulnerabilities and unpatched software. APT groups leverage this type of attack to target healthcare entities. Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. By targeting SSO applications, malicious actors hope to maximize access to intellectual property during a successful compromise.

- **Targeting** email applications. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud, (2) subsequently download user mail to locally stored email files, (3) identify the entire company's email address list, and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.

- **TTPs of password spraying include:**
  - Using social engineering tactics to perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray.
  - Using easy-to-guess passwords (e.g., "Winter2018", "Password123!") and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
  - Leveraging the initial group of compromised accounts, downloading the Global Address List (GAL) from a target's email client, and performing a larger password spray against legitimate accounts
  - Using the compromised access, attempting to expand laterally (e.g., via Remote Desktop Protocol) within the network, and performing mass data exfiltration using File Transfer Protocol tools such as FileZilla

1 CISA. (May 6, 2020). Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/TA18-086A

TTPs

Drive-by Compromise[1]

- A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring application access tokens.

Exploit Public-Facing Application[2]

- The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

External Remote Services[3]

- Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.

1 MITRE. (October 11, 2019). Drive-by Compromise. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1189/
2 MITRE. (October 22, 2019). Exploit Public-Facing Application. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1190/
3 MITRE. (May 31, 2017). External Remote Services. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1133/

TTPs

Hardware Additions[1]

- Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping, man-in-the middle encryption breaking, keystroke injection, kernel memory reading via DMA, adding new wireless access to an existing network, and others.

Replication Through Removable Media[2]

- Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

Spearphishing Attachment[3]

- Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

1 MITRE. (July 17, 2019). Hardware Additions. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1200/
2 MITRE. (July 18, 2019). Replication Through Removable Media. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1091/
3 MITRE. (June 24, 2019). Spearphishing Attachment. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1193/

TTPs

Spearphishing Link[1]

- Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

Spearphishing via Service[2]

- Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

Supply Chain Compromise[3]

- Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Trusted Relationship[4]

- Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

11 MITRE. (October 18, 2019). Spearphishing Link. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1192/
2 MITRE. (June 24, 2019). Spearphishing via Service. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1194/
3 MITRE. (June 21, 2019). Supply Chain Compromise. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1195/
4 MITRE. (October 11, 2019). Trusted Relationship. Accessed May 13, 2020 at: https://attack.mitre.org/techniques/T1199/

Malware

Name	Type	Description
Emotet (1) (2)	Trojan that is primarily spread through spam emails. The infection may arrive either via malicious script, macro-enabled document files, or malicious link and contain familiar branding designed to look like a legitimate email.	An advanced, modular trojan that primarily functions as a downloader or dropper of other trojans. Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.
TrickBot (1) (3)	Trojan developed in 2016 used to target Windows machines.	A modular trojan that targets sensitive information and acts as a dropper for other malware. Since June 2019, the MS-ISAC observed an increasingly close relationship between initial TrickBot infections and eventual Ryuk ransomware attacks.
Ryuk (1) (4)	Ransomware that uses encryption to block access to a system, device, or file until a ransom is paid.	A type of crypto-ransomware that uses encryption to block access to a system, device, or file until a ransom is paid. Ryuk is often dropped on a system by other malware, most notably TrickBot.

1. Malwarebytes, (November 2019) CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE, https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
2. Cyber Infrastructure Security Agency, (July 20,2018), ALERT (TA18-201A) EMOTET MALWARE, https://www.us-cert.gov/ncas/alerts/TA18-201A
3. Multistate Information Sharing and Analysis Center, (September, 2019) SECURITY PRIMER TRICKBOT (SP2019-0962), https://protect2.fireeye.com/url?k=cd32461b-91674f08-cd327724-0cc47adb5650-72e3e3124a28231d&u=http://www.cisecurity.org/white-papers/security-primer-trickbot/
4. Shyum Oza, Spanning Blog, (January 24, 2020) RYUK RANSOMWARE – MALWARE OF THE MONTH, JANUARY 2020 https://protect2.fireeye.com/url?k=7258e3ba-2e0deaa9-7258d285-0cc47adb5650-3b1332e606fb2fa7&u=https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/

Malware

Name	Type	Description
MAZE (5)	Ransomware that not only uses encryption to block access to a system, device, or file until a ransom is paid but renames files and often releases some information as an incentive for payment.	Deploys ransomware post-compromise. This methodology provides an opportunity to infect more hosts within a victim's environment and exfiltrate data, which is leveraged to apply additional pressure on organizations to pay extortion fees. Notably, in at least some cases, the actors behind these operations charge an additional fee, in addition to the decryption key, for the non-release of stolen data.
Gh0st Rat (6)	Trojan "Remote Access Tool" used on Windows platforms	A family of backdoors, or more accurately, remote administration tools (RATs), used to gain control of the computer it infects. It is affiliated with Ghostnet bot network, and steals information by logging keystrokes.

5. Xtelligent Healthcare Media, Health IT Security, (January 7, 2020) FBI ALERTS TO RISE IN MAZE RANSOMWARE, EXTORTION ATTEMPTS https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts
6. RSA, (April, 2018),GH0ST RAT: COMPLETE MALWARE ANALYSIS - PART 1 https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/

Vulnerabilities

CVE-2015-1641

- **Vulnerable Products:** Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1
- **Associated Malware**: Toshliph, Uwarrior
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2015-1641
- **IOCs:** https://www.us-cert.gov/ncas/analysis-reports/ar20-133m

CVE-2017-8759

- **Vulnerable Products:** Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7
- **Associated Malware:** FINSPY, FinFisher, WingBird
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2017-8759
- **IOCs:** https://www.us-cert.gov/ncas/analysis-reports/ar20-133f

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Vulnerabilities

CVE-2017-0143

- **Vulnerable Products:** Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016
- **Associated Malware:** Multiple using the EternalSynergy and EternalBlue Exploit Kit
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2017-0143

CVE-2017-8759

- **Vulnerable Products:** Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7
- **Associated Malware:** FINSPY, FinFisher, WingBird
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2017-8759
- **IOCs:** https://www.us-cert.gov/ncas/analysis-reports/ar20-133f

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Vulnerabilities

CVE-2017-11882

- **Vulnerable Products:** Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 Products
- **Associated Malware:** Loki, FormBook, Pony/FAREIT
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2017-11882
- **IOCs:** https://www.us-cert.gov/ncas/analysis-reports/ar20-133e

CVE-2017-0199

- **Vulnerable Products:** Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016, Vista SP2, Server 2008 SP2, Windows 7 SP1, Windows 8.1
- **Associated Malware**: FINSPY, LATENTBOT, Dridex
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2017-0199
- **IOCs:**
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133g
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133h
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133p

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Vulnerabilities

CVE-2017-5638

- **Vulnerable Products:** Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1
- **Associated Malware:** JexBoss
- **Mitigation:** Upgrade to Struts 2.3.32 or Struts 2.5.10.1
- **More Detail:**
  - https://www.us-cert.gov/ncas/analysis-reports/AR18-312A
    https://nvd.nist.gov/vuln/detail/CVE-2017-5638

CVE-2018-4878

- **Vulnerable Products**: Adobe Flash Player before 28.0.0.161
- **Associated Malware:** DOGCALL
- **Mitigation:** Update Adobe Flash Player installation to the latest version
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2018-4878
- **IOCs**: https://www.us-cert.gov/ncas/analysis-reports/ar20-133d

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Vulnerabilities

CVE-2012-0158

- **Vulnerable Products:** Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0

- **Associated Malware:** Dridex

- **Mitigation:** Update affected Microsoft products with the latest security patches

- **More Detail:**
  - https://www.us-cert.gov/ncas/alerts/aa19-339a
  - https://nvd.nist.gov/vuln/detail/CVE-2012-0158

- **IOCs:**
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133i
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133j
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133k
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133l
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133n
  - https://www.us-cert.gov/ncas/analysis-reports/ar20-133o

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Vulnerabilities

CVE-2019-0604

- **Vulnerable Products:** Microsoft SharePoint
- **Associated Malware:** China Chopper
- **Mitigation:** Update affected Microsoft products with the latest security patches
- **More Detail:**
  - https://nvd.nist.gov/vuln/detail/CVE-2019-0604

CVE-2018-7600

- **Vulnerable Products:** Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1
- **Associated Malware:** Kitty
- **Mitigation:** Upgrade to the most recent version of Drupal 7 or 8 core.
- **More Detail:** https://nvd.nist.gov/vuln/detail/CVE-2018-7600

CVE-2019-11510

- **Vulnerable Products:** Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 and Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15
- **Mitigation:** Update affected Pulse Secure devices with the latest security patches.
- **More Detail:**
  - https://www.us-cert.gov/ncas/alerts/aa20-107a
  - https://nvd.nist.gov/vuln/detail/CVE-2019-11510
  - https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

CVE-2019-19781

- **Vulnerable Products:** Citrix Application Delivery Controller, Citrix Gateway, and Citrix SDWAN WANOP
- **Mitigation:** Update affected Citrix devices with the latest security patches
- **More Detail:**
  - https://www.us-cert.gov/ncas/alerts/aa20-020a
  - https://www.us-cert.gov/ncas/alerts/aa20-031a
  - https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html
  - https://nvd.nist.gov/vuln/detail/CVE-2019-19781
  - https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

CISA. (May 12, 2020). Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities. Accessed on May 18, 2020 at: https://www.us-cert.gov/ncas/alerts/aa20-133a

Recommendations and Mitigations

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are examples from HICP that can be used to mitigate some common threats.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

HHS. (December 28, 2018). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Accessed June 4, 2020 at: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Recommendations and Mitigations

Security Operations &Threat Intelligence

- Set up a security monitoring capability so you are collecting the data that will be needed to analyze network intrusions.
- Understand APT and associated cybercriminals tactics, techniques, and procedures (TTPs) to include, historical attacks and targeted vulnerabilities.
- Increase the identification and ingestion of APT and associated cybercriminal unit IOCs.

Patch Management

- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and configurations. See CISA's guidance on enterprise VPN security and NCSC guidance on virtual private networks for more information.
- Keep systems updated with the most recent patches and prioritize patching for the most at-risk systems based on identified TTPs.

CISA. (May 5, 2020). APT Groups Target Healthcare and Essential Services. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/AA20126A.
NCSC. (May 15, 2018). Spray you, spray me: defending against password spraying attacks. Accessed May 13, 2020 at: https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks. vi CISA. (March 27, 2018). Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/TA18-086A.

Recommendations and Mitigations

Assets

- Use modern systems and software.
- If you cannot move off out-of-date platforms and applications, there are short-term steps you can take to improve your position.

Architecture

- Protect the management interfaces of your critical operational systems.
- In particular, use browse-down architecture to prevent attackers easily gaining privileged access to your most vital assets.

Incident Response

- Have and practice an incident response plan. Identify which events are considered incidents and provide organizational structure, roles, and responsibilities for responding to these events.
- Develop procedures for performing incident handling and reporting. Set guidelines for communicating with outside parties regarding incidents.

CISA. (May 5, 2020). APT Groups Target Healthcare and Essential Services. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/AA20126A
Scholl, M., Kevin Stine, Kenneth Lin, & Daniel Steinberg. (September 2010). Security Architecture Design for Health Information Exchanges (HIEs). NIST. Accessed May 13, 2020 at: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7497.pdf
EAC. (n.d.) Cyber Incident Response Best Practices. US Election Assistance Comission. Accessed May 13, 2020 at: https://www.eac.gov/sites/default/files/eac_assets/1/6/Incident-Response_best-practices.pdf

Recommendations and Mitigations

Passwords

- Review password policies to ensure they align with the latest NIST guidelines, and deter the use of easy-to-guess passwords.
- Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap.
- Regularly audit user passwords against common password lists, using free or commercial tools.
- Provide pragmatic advice to users on how to choose good passwords.

Authentication

- Enable multi-factor authentication (MFA), and review MFA settings to ensure coverage on externally-reachable endpoints.

Training

- Understanding Cognitive Bias
- The Need for Controls
  - Administrative
    - Roles, Responsibilities, Functions
    - Separation of Duties
  - Physical and Process
    - Physical protections
    - Protective procedures
    - Principle of Least Privilege
- Cyber Hygiene / Awareness
  - Social Engineering
  - Protective Procedures

CISA. (May 5, 2020). APT Groups Target Healthcare and Essential Services. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/AA20126A.
NCSC. (May 15, 2018). Spray you, spray me: defending against password spraying attacks. Accessed May 13, 2020 at: https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks. vi CISA. (March 27, 2018). Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors. Accessed May 13, 2020 at: https://www.us-cert.gov/ncas/alerts/TA18-086A.

Summary

- APT groups steal data, disrupt operations, and destroy infrastructure. Unlike most cybercriminals, APT attackers pursue their objectives over longer periods of time. They adapt to cyber defenses and frequently retarget the same victim.
- Common HPH targets include:
  - Healthcare
  - Biotechnology
  - Medical devices
  - Pharmaceuticals
  - Healthcare information technology
  - Scientific research
- HPH organizations who have been victim of APT attacks have suffered:
  - Reputational harm
  - Disruption to operations
  - Financial losses
  - PII/PHI and proprietary data theft
- HC3 recommends several mitigations and controls to counter APT threats.

Questions

Reference Materials

References

- CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE
  - https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
- ALERT (TA18-201A) EMOTET MALWARE
  - https://www.us-cert.gov/ncas/alerts/TA18-201A
- SECURITY PRIMER TRICKBOT
  - www.cisecurity.org/white-papers/security-primer-trickbot/
- RYUK RANSOMWARE – MALWARE OF THE MONTH, JANUARY 2020
  - https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/
- A ONE-TWO PUNCH OF EMOTET, TRICKBOT, & RYUK STEALING & RANSOMING DATA
  - https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data
- EMOTET
  - https://www.malwarebytes.com/emotet/
- FBI ALERTS TO RISE IN MAZE RANSOMWARE, EXTORTION ATTEMPTS
  - https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts
- GH0ST RAT: COMPLETE MALWARE ANALYSIS - PART 1
  - https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/
- GROUPS
  - https://attack.mitre.org/groups/
- ADVANCED PERSISTENT THREAT GROUPS
  - https://www.fireeye.com/current-threats/apt-groups.html

References

- THE ANTHEM HACK: ALL ROADS LEAD TO CHINA
  - https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/
- THREATCONNECT PROVIDES A REPORT ON HEALTHCARE AND MEDICAL INDUSTRY THREATS
  - https://threatconnect.com/blog/protecting-medical-healthcare-organizations/
- HOW CHINA'S ELITE HACKERS STOLE THE WORLDS MOST VALUABLE SECRETS
  - https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/
- NEW ORANGEWORM ATTACK GROUP TARGETS THE HEALTHCARE SECTOR IN THE US, EUROPE, AND ASIA
  - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
- RUSSIA'S ELITE HACKING UNIT HAS BEEN SILENT, BUT BUSY
  - https://www.zdnet.com/article/russias-elite-hacking-unit-has-been-silent-but-busy/
- CYBER INCIDENT RESPONSE BEST PRACTICES
  - https://www.eac.gov/sites/default/files/eac_assets/1/6/Incident-Response_best-practices.pdf
- DEEP PANDA
  - https://attack.mitre.org/groups/G0009/
- FIN4
  - https://attack.mitre.org/groups/G0085/
- COMMUNITY HEALTH SYSTEMS CYBER ATTACK PUTS 4.5M PATIENTS AT RISK
  - https://www.hipaajournal.com/community-health-systems-cyber-attack-puts-4-5m-patients-risk/

References

- APT18
  - https://attack.mitre.org/groups/G0026/
- THREAT RESEARCH: DEMONSTRATING HUSTLE, CHINESE APT GROUPS QUICKLY USE ZERO-DAY VULNERABILITY (CVE-2015-5119) FOLLOWING HACKING TEAM LEAK
  - https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html
- BEYOND COMPLIANCE: CYBER THREATS AND HEALTHCARE
  - https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare
- MANDIANT: APT 1 EXPOSING ONE OF CHINA'S ESPIONAGE UNITS
  - https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
- ALERT (AA20-126A) APT GROUPS TARGET HEALTHCARE AND ESSENTIAL SERVICES
  - https://www.us-cert.gov/ncas/alerts/AA20126A
- 83% OF MEDICAL DEVICES RUN ON OUTDATED OPERATING SYSTEMS
  - https://www.hipaajournal.com/83-of-medical-devices-run-on-outdated-operating-systems/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- APT10 (MENUPASS GROUP): NEW TOOLS, GLOBAL CAMPAIGN LATEST MANIFESTATION OF LONGSTANDING THREAT
  - https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
- NEW ORANGEWORM ATTACK GROUP TARGETS THE HEALTHCARE SECTOR IN THE US, EUROPE, AND ASIA
  - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

References

- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- APT10 (MENUPASS GROUP): NEW TOOLS, GLOBAL CAMPAIGN LATEST MANIFESTATION OF LONGSTANDING THREAT
  - https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
- APT29
  - https://attack.mitre.org/groups/G0016/
- ALERT (AA20-133A) TOP 10 ROUTINELY EXPLOITED VULNERABILITIES
  - https://www.us-cert.gov/ncas/alerts/aa20-133a
- CYBER INCIDENT RESPONSE BEST PRACTICES
  - https://www.eac.gov/sites/default/files/eac_assets/1/6/Incident-Response_best-practices.pdf
- SPRAY YOU, SPRAY ME: DEFENDING AGAINST PASSWORD SPRAYING ATTACKS
  - https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks
- COVID19 RELATED NATION-STATE AND CYBER CRIMINAL TARGETING OF THE HEALTHCARE SECTOR
  - www.aha.org/other-cybersecurity-reports/2020-05-18-hc3-threat-brief-tlp-white-covid-19-related-nation-state-and
- ALERT (TA18-086A) BRUTE FORCE ATTACKS CONDUCTED BY CYBER ACTORS
  - https://www.us-cert.gov/ncas/alerts/TA18-086A
- NISTSIR 7497 SECURITY ARCHITECTURE DESIGN PROCESS FOR HEALTH INFORMATION EXCHANGES (HIE)
  - https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7497.pdf

References

- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE
  - https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
- ALERT (TA18-201A) EMOTET MALWARE
  - https://www.us-cert.gov/ncas/alerts/TA18-201A
- MS-ISAC RELEASES SECURITY PRIMER ON TRICKBOT MALWARE
  - https://www.us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware
- RYUK RANSOMWARE – MALWARE OF THE MONTH JANUARY 2020
  - https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/
- MITRE ATT&CK MATRICES
  - https://attack.mitre.org/matrices/enterprise/
- FBI ALERTS TO RISE IN MAZE RANSOMWARE, EXTORTION ATTEMPTS
  - https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts
- GH0ST RAT: COMPLETE MALWARE ANALYSIS – PART I
  - https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/

References

- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE
  - https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
- ALERT (TA18-201A) EMOTET MALWARE
  - https://www.us-cert.gov/ncas/alerts/TA18-201A
- MS-ISAC RELEASES SECURITY PRIMER ON TRICKBOT MALWARE
  - https://www.us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware
- RYUK RANSOMWARE – MALWARE OF THE MONTH JANUARY 2020
  - https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/
- MITRE ATT&CK MATRICES
  - https://attack.mitre.org/matrices/enterprise/
- FBI ALERTS TO RISE IN MAZE RANSOMWARE, EXTORTION ATTEMPTS
  - https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts
- GH0ST RAT: COMPLETE MALWARE ANALYSIS – PART I
  - https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/

References

- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- CYBERCRIME TACTICS AND TECHNIQUES: THE 2019 STATE OF HEALTHCARE
  - https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
- ALERT (TA18-201A) EMOTET MALWARE
  - https://www.us-cert.gov/ncas/alerts/TA18-201A
- MS-ISAC RELEASES SECURITY PRIMER ON TRICKBOT MALWARE
  - https://www.us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware
- RYUK RANSOMWARE – MALWARE OF THE MONTH JANUARY 2020
  - https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/
- MITRE ATT&CK MATRICES
  - https://attack.mitre.org/matrices/enterprise/
- FBI ALERTS TO RISE IN MAZE RANSOMWARE, EXTORTION ATTEMPTS
  - https://healthitsecurity.com/news/fbi-alerts-to-rise-in-maze-ransomware-extortion-attempts
- GH0ST RAT: COMPLETE MALWARE ANALYSIS – PART I
  - https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/
- APT GROUP EXPLOITING HACKING TEAM FLASH ZERO DAY
  - https://threatpost.com/apt-group-exploiting-hacking-team-flash-zero-day/113715/

References

- Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors
  - https://www.us-cert.gov/ncas/alerts/TA18-086A

- MITRE ATT&CK Enterprise Techniques
  - https://attack.mitre.org/techniques/enterprise/

Questions

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV