LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Intelligence Briefing Update Ransomware Threat to State & Local Governments

OVERALL CLASSIFICATION IS

UNCLASSIFIED

TLP:WHITE

5/30/2019

Agenda

The Ransomware Threat to State & Local Government

- Overview
  - The Trend – targeted or opportunistic?
  - Why Target State & Local Government?
  - Early Examples
- Operational Impacts – Direct and Indirect
  - Link to Healthcare
- Exposure to Common Attack Vectors -- EternalBlue
  - Baltimore
  - Public Schools / Education
- Examples
  - Matanuska-Susitna (Anchorage, AK)
- Ransomware Trends
  - Post-Compromise Deployment
  - RobbinHood Ransomware
- Protection / Detection
- Conclusion

Slides Key:

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

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

Overview

The Ransomware Threat to State & Local Governments (Recorded Future)

- An observed uptick in cyberattacks (mostly ransomware) targeting the essential networks, infrastructure and services of cities, municipalities and local governments in the US
- According to publicly reported ransomware events, ransomware has hit 48 states and the District of Columbia
- Based on analysis of publicly reported ransomware events since 2016…
  - Direct/indirect impacts on Healthcare & Public Health (HPH) sector
  - These environments threatened by emerging / popular ransomware
  - Reflects trends in ransomware attacks across all sectors
  - Shows a recent uptick in these attacks

Ryuk / SamSam / GandCrab ransomware families

Drop in frequency of attacks from ~late 2016 to ~early 2018

22+ (and likely more) in Q1 2019, on pace for record year

Why Target State & Local Governments?

- Often softer targets than some of the better-equipped enterprise networks
- Store highly valuable information about individuals and critical infrastructure, facilitate financial transactions
- Generate a lot of media coverage because of the effect these attacks have on the functioning of essential infrastructure and processes
  - This likely creates a perception among attackers that these are potentially profitable targets
  - Raises attacker's profile → likely response from law enforcement / FBI to assist with investigations

Minerva-Labs

Overview

Overview and Trend of Targeting State & Local Governments

Based on Public Reporting…

- Since 2013 → 169 ransomware incidents affecting State & Local Governments
  - 24 of the 169 attacks were against local school systems or colleges
  - 41 of the 169 attacks were against law enforcement offices
  - 40 of the 169 (only) reported incidents identified the type of ransomware, but generally depict the overall trend in popular / active ransomware families:

2013-2016	Cryptolocker Cryptowall
2017-2018	WannaCry SamSam
2018-2019	GandCrab Ryuk

- The number of publicly reported ransomware events since 2016 reflects the trends in ransomware attacks for all sectors, as well as a recent uptick:

2016	2017	2018	2019 First Quarter (Q1)
46 ransomware attacks	38 ransomware attacks	53 ransomware attacks	21 ransomware attacks

Reflective of the drop in ransomware attacks across all sectors

On pace for 84 ransomware attacks on such environments in 2019

The attacks appear more opportunistic than deliberate

- "[Once] these groups do realize they are in a state or local government target, they take advantage of the fact by targeting the most sensitive or valuable data to encrypt" (statescoop)

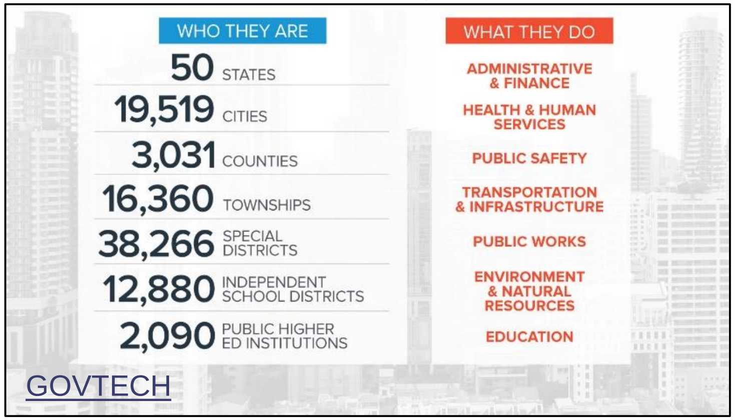
Recorded Future

Overview - Impacts

Impact on Healthcare and Public Health (HPH) Sector (ITSP Mag)

What entities fall under State & Local Government?

- Health and Human Services
- Public Safety programs
- Transportation and Infrastructure (initiatives and maintenance)
- Schools / Education



WHO THEY ARE

50	STATES
19,519	CITIES
3,031	COUNTIES
16,360	TOWNSHIPS
38,266	SPECIAL DISTRICTS
12,880	INDEPENDENT SCHOOL DISTRICTS
2,090	PUBLIC HIGHER ED INSTITUTIONS

WHAT THEY DO

- ADMINISTRATIVE & FINANCE
- HEALTH & HUMAN SERVICES
- PUBLIC SAFETY
- TRANSPORTATION & INFRASTRUCTURE
- PUBLIC WORKS
- ENVIRONMENT & NATURAL RESOURCES
- EDUCATION

GOVTECH

Operational Impacts on Local Governments / Municipalities

- For local governments and municipalities, economies and public welfare are tied to the ability to access data, services and applications
  - Ransomware attacks can disrupt all citizen-facing services and operations.
- Risk of losing control of / access to confidential and personal information (Social Security numbers (SSN) and credit card information/payment data)
- Locking up payment platforms or portals could effectively cease municipal operations
  - Ransomware has previously shut down 911 and 311 dispatch systems (potentially putting lives at risk) (tml1)

EXAMPLE:

March 2018 → ransomware attack on Baltimore shut down the computer-aided dispatch (CAD) system

- for about 22 hours impacting the 911 system. While manual dispatching enabled public safety officers to respond to calls during this time period, the city’s dispatch calls were not recorded.

Tennessee Municipal League

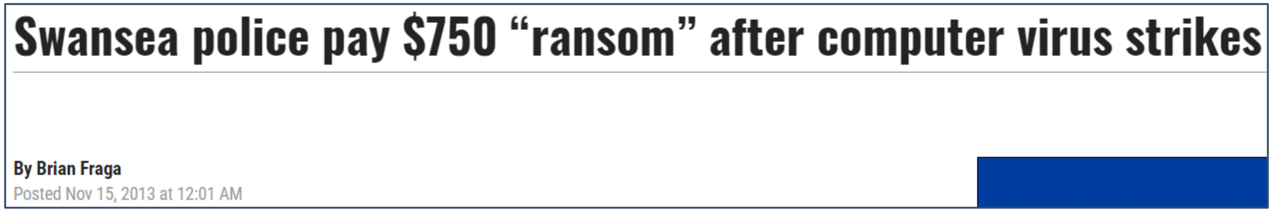
Overview - Impacts

History of Ransomware Attacks on State & Local Government

The early examples of attacks:

Swansea Police Department (MA) → November 2013 (Herald News)

- Ransomware used: CryptoLocker
- Impact: encryption of numerous images and Word documents
- Ransom paid: $750 (2 Bitcoin)



Swansea police pay $750 "ransom" after computer virus strikes

By Brian Fraga

Posted Nov 15, 2013 at 12:01 AM

Greenland, New Hampshire → December 2013 (Aberdeen)

- Ransomware used: CryptoLocker
- Impact: Town Hall computers infected
  - Eight years worth of documents gone
- Ransom not paid: missed 100 hour timeline to pay $300 in Bitcoin

Impacts – Direct and Indirect

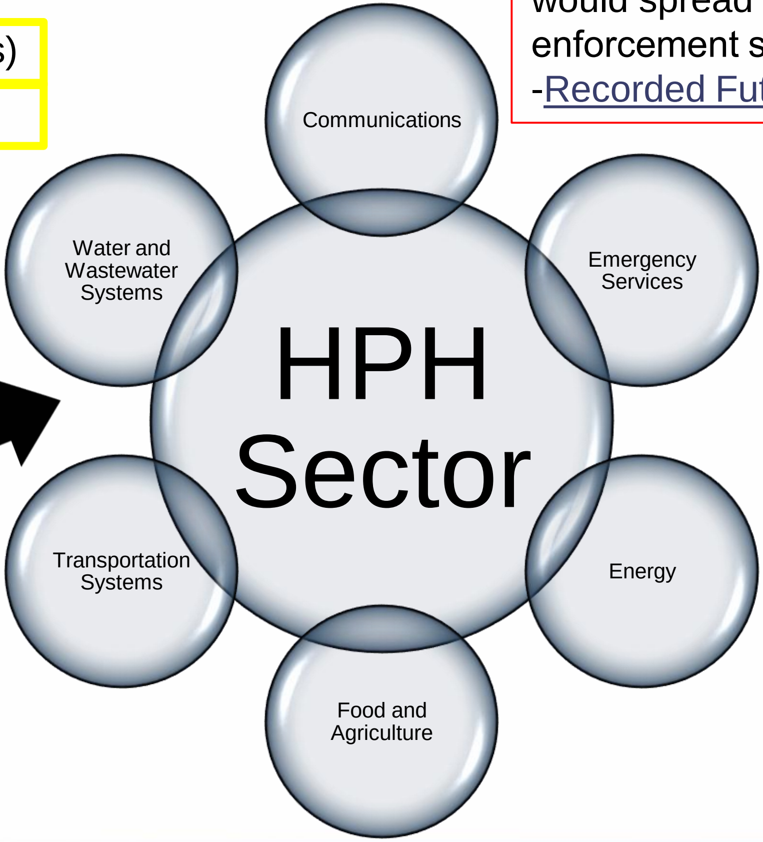
Potential Impacted Services of State and Local Governments:

- Law enforcement (dispatch, 911, public safety programs)
- Education / school networks
- Payment portals
- Emergency services (EMS, fire departments)
- Transportation / transit services
- Water / sewage
- Power / electricity
- State Agencies
- Food & Agriculture

> "There is some overlap because several attacks that started with local government computers would spread to law enforcement systems as well."
> -Recorded Future

Impact on the HPH Sector

Interdependencies →
"The Healthcare and Public Health Sector is highly dependent on fellow sectors for continuity of operations and service delivery"



DHS

Examples

Examples of Ransomware hitting State & Local Government Infrastructure

May 2019: Baltimore (MSSP Alert Baltimore)

PC and server issues: 10,000 city government computers frozen.

Real estate transactions: Roughly 200 to 300 closings were delayed because the city couldn't tell title insurers whether the seller had any unpaid liens.

Public Health Systems: Baltimore's health department couldn't access the state network that helps them warn the public when bad batches of street drugs trigger overdoses.

City Utilities: The city's public-works department couldn't generate new water bills for customers, which could mean residents will get unusually high bills once the problem is fixed

April 2019: Cleveland Hopkins International Airport suffered a ransomware attack (municipality owned)

April 2019: Augusta, Maine, suffered a highly targeted ransomware attack that froze the city's entire network and forced the city center to close

March 2019: Albany, New York, suffered a ransomware attack

March 2019: Jackson County, Georgia officials paid cybercriminals $400,000 after a cyberattack shut down the county's computer systems

March 2018: Atlanta, Georgia suffered a major ransomware attack.

February 2018: Colorado Department of Transportation (CDOT) employee computers temporarily were shut down due to a SamSam ransomware attack.

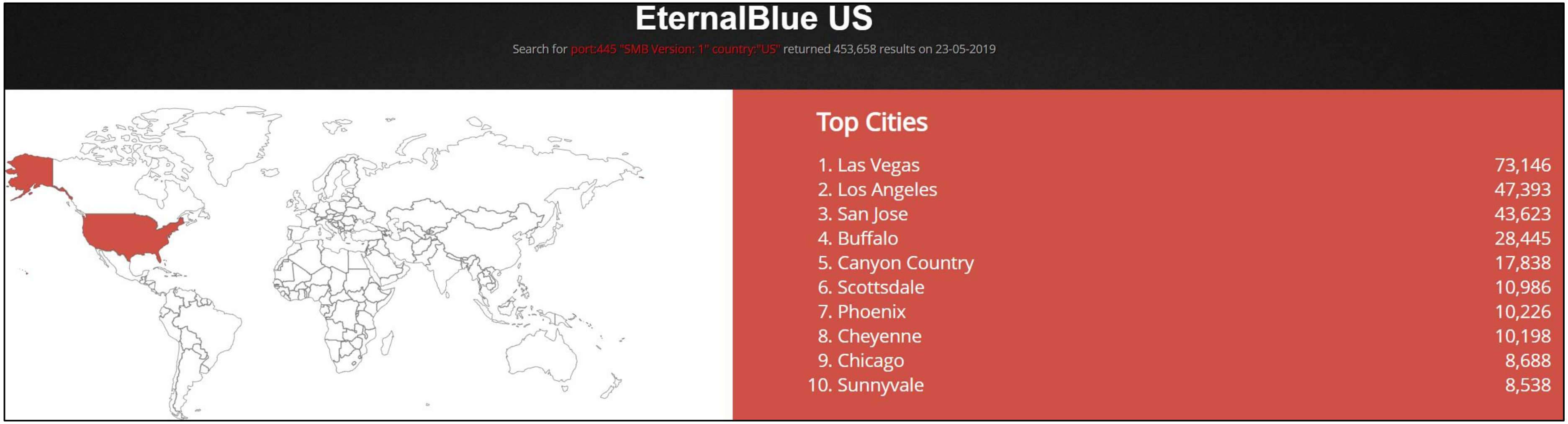
MSSP Alert

Exposure to Common Attacks

TLP:WHITE

EternalBlue (WannaCry) → United States (Shodan Report)

- Over 450,000 public-facing US servers, open port 445, running SMB Version 1 (vulnerable to EternalBlue)



EternalBlue US

Search for port:445 "SMB Version: 1" country:"US" returned 453,658 results on 23-05-2019

Top Cities

1. Las Vegas	73,146
2. Los Angeles	47,393
3. San Jose	43,623
4. Buffalo	28,445
5. Canyon Country	17,838
6. Scottsdale	10,986
7. Phoenix	10,226
8. Cheyenne	10,198
9. Chicago	8,688
10. Sunnyvale	8,538

New York Times Report (NYT):

Threat actors leveraged EternalBlue exploit in attack against Baltimore city government

EternalBlue (WannaCry) → Baltimore

- The same search, with filter city:“Baltimore”, had 131 results

Public Schools

Who Oversees Public Schools and Districts

The governance of public schools is a rather complex issue that incorporates various government entities at the federal, state and local levels (Public School Review)

State Governance

- Providing and allocating funding for public schools
- Setting state standards for assessments, standards and curriculum
- Overseeing special services for students with disabilities or other challenges

Local Oversight

- Oversight and development of school policies within their district
- Adoption of the school budget and allocation of resources
- Employment of district superintendent

For tax purposes, public schools are considered a part of the local government (Intuit)

- Anyone that works for the school district is considered an employee of a local government
- Public schools are funded by local taxes and are run by elected officials

School infrastructure is a significant concern in ransomware attacks
-Schools are often impacted in ransomware attacks on both local and state government entities
-Schools are exposed to common attacks vectors observed in ransomware campaigns

Exposure → Schools

Schools Remain Vulnerable

Schools, including those in large districts, remain vulnerable and exposed to common attack vectors

- Based on Shodan search results… (Ars)
  - Potentially thousands of the EternalBlue vulnerable servers in the US (450,000+) are in use at public school systems across the US
  - In Baltimore, EIGHT publicly accessible servers vulnerable to EternalBlue
  - This includes cases where the patch has been applied, because some vendors still require the protocol for applications such as networked copiers and scanners

Some of the other districts hosting the largest number of potentially vulnerable systems include:

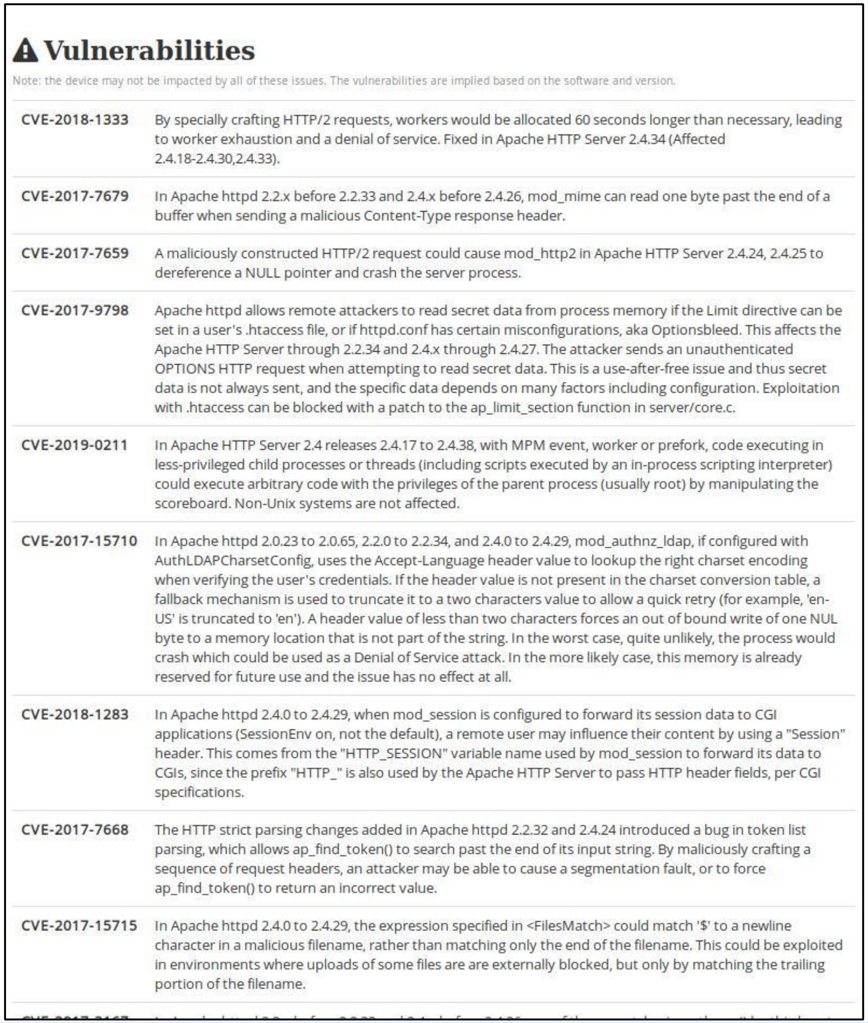
- The Montebello Unified School District in Los Angeles County, California
- Fresno Unified School District in Fresno, California
- The Washington School Information Processing Cooperative in the state of Washington
- Cupertino Union School District in San Jose, California

Ars

Exposure to Common Attacks

EternalBlue (WannaCry) → California County School

- According to research by @thepacketrat
- Using relatively common scanning tools Shodan and Nmap (Network Mapper)
- It was discovered that a school in an unidentified California county has an open RDP server
- Server location was the superintendent’s office
- Numerous associated vulnerabilities



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-1333	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-7659	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

Ars

Examples

Matanuska-Susitna (Mat-Su) (Bleeping Computer)

- Mat-Su is a borough part of the Anchorage Metropolitan Statistical Area
- July 24, 2018: Bitpaymer ransomware deployed on network

Impact on Mat-Su Services (Mat-Su IT Director)

- Nearly all of the 500 workstations (both Windows 7 and Windows 10) and 120 of the 150 servers have been infected.
- Almost all Windows based production servers have been encrypted, including their domain, SharePoint (intranet and eCommerce), SQL databases, S:\ drive files shares (L:\, M:\, P:\ ) and the backup and Disaster Recovery (DR) servers
- The phone system (Mitel) was encrypted → some functionality lost
- The door lock card swipe system (Lenel) was encrypted → continued to function in last known good condition
- Email (Exchange) completely unrecoverable.

4 to 6 weeks prior to ransomware deployment

- Emotet (likely) lying dormant within the system
- Represents the trend in post-compromise ransomware deployment

Mat-Su IT Director

Post-Compromise Deployment

Post-Compromise Deployment of Ransomware

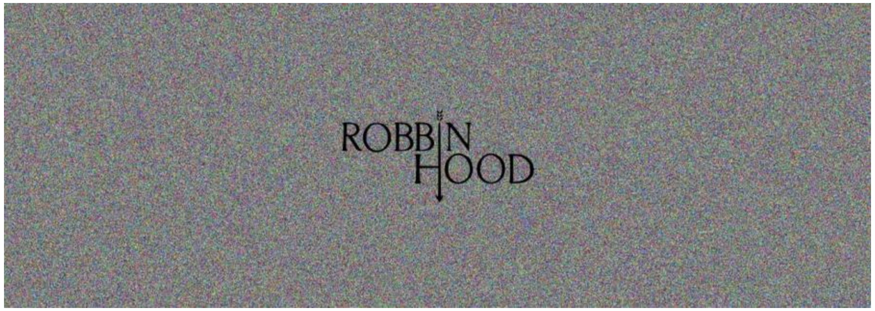
- "When [ransomware attackers] infect a new victim, they can stay for a while to observe the network ... and see if the infected machine or network is interesting"
- "They do not automatically drop [the ransomware]; they drop it manually" if they decide it's a useful target
- This is a newer trend and a departure from earlier ransomware attack campaigns that were more random and automated

Trojans (Loaders) Preceding Ransomware

- Attacks using ransomware-as-a-service (RaaS) platforms remain commonplace (Insurance Journal)
  - These tend to hit unsuspecting small businesses and individuals at random
- INCREASE in attacks using (arguably) more sophisticated ransomware variants are being deployed through phishing emails and trick users into activating banking Trojans, loaders
- Banking Trojans such as Emotet and Trickbot have been used by criminals to harvest all kinds of account details, and newer types of banking Trojans will also perform reconnaissance on email accounts and deploy other malware, most commonly ransomware, onto a system with relative ease

DARKReading

RobbinHood Ransomware



ROBBINHOOD RANSOMWARE (Bleeping Computer)

- **First observed:** April 2019
- **Written in:** Go programming

Confirmed in two attacks on State & Local government:

- Baltimore, Maryland
- City of Greenville, North Carolina

- **Capabilities** include disabling services, deleting volume shadow copies, killing processes, and clearing Windows event logs.
- **Post-Compromise Deployment**
  - Not distributed through spam → hacked remote desktop services (RDS) or other Trojans that provide access to the attackers, such as Emotet or Trickbot
- **Disconnects all network shares from the computer using the command:** cmd.exe /c net use * /DELETE /Y
  - This means that each computer is targeted individually and that other computers are not encrypted via connected shares
  - This could also indicate that the payload is being pushed to each individual machine via a domain controller or through a framework like Empire PowerShell and PSExec.

Protection / Detection

General Ransomware Protection (Trend Micro)

- Regularly back up files and ensure their integrity and availability.
- Keep the operating system, servers, networks, and endpoints patched to deter attacks that exploit security gaps
- Disable or restrict and secure the use of system administration tools that may be abused.
- Set up security mechanisms at all levels of the organization’s online infrastructure: data categorization, network segmentation, application control/whitelisting, and behavior monitoring help mitigate further exposure and thwart suspicious files and anomalous activities within the system from being carried out.
- Enable the firewall, sandbox, as well as intrusion detection and prevention systems.

RobbinHood Ransomware Indicators of Compromise (IOC)

797f2e939bf396e50defa14240491684

73d43cf4aecf2dc55ef61ab17dfbb147

A6d61654e6af6f1fa417229aa2da76f2

Edfec708d2b6686beb55e449fb55d11e

Aace43af8d0932a7b01c5b8fb71c8199

5c9c205c7767472abb8bc112f79afd7e

d80a899168e859c4daea95b64f90645c

Protection / Detection

TLP:WHITE

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Membership includes all 50 States and over 1000 local government organizations, U.S. territories and tribal nations
- Shares security incident information and analysis
- Runs a 24-hour watch and warning security operations center

If there is a suspected or confirmed cyber incident that…

- Affects core government functions;
- Affects critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems; or
- Indicates malicious software is present on critical systems

CONTACT MS-ISAC:

(866) 787-4722

soc@msisac.org

EAC

Questions

Upcoming Briefs

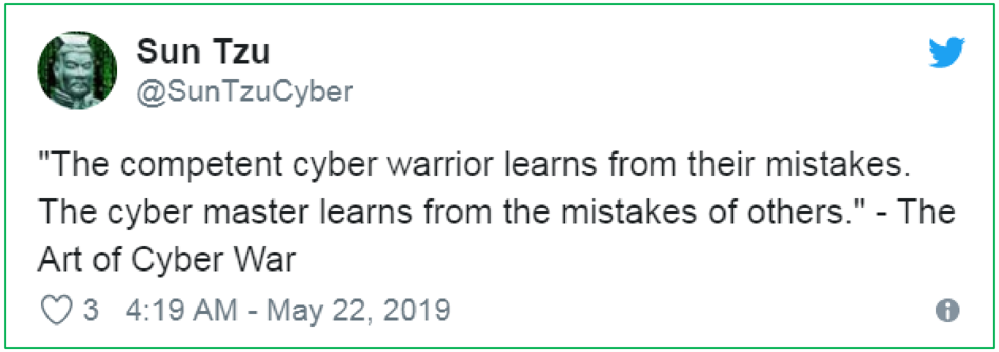
- Vulnerability/Patch Management for the Healthcare Enterprise

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.**



Sun Tzu
@SunTzuCyber

"The competent cyber warrior learns from their mistakes. The cyber master learns from the mistakes of others." - The Art of Cyber War

♡ 3 4:19 AM - May 22, 2019