# Report on Ongoing SamSam Ransomware Campaigns
# Date: 03/30/2018

**Healthcare Cybersecurity and Communications Integration Center (HCCIC)**
HHSHCCIC@HHS.GOV

## SUMMARY:

In 2018, there have been at least eight separate cyber-attacks on healthcare and government organizations utilizing a form of ransomware known as SamSam:

- two Indiana based hospitals
- a cloud-based Electronic Health Record (EHR) provider
- a New Mexico Municipality computer system
- an unnamed ICS (Industrial Control Systems) company in the US.[i]
- Davidson County in North Carolina
- Colorado's Department of Transportation (CDOT) – *twice*
- Systems and services in Atlanta, Georgia

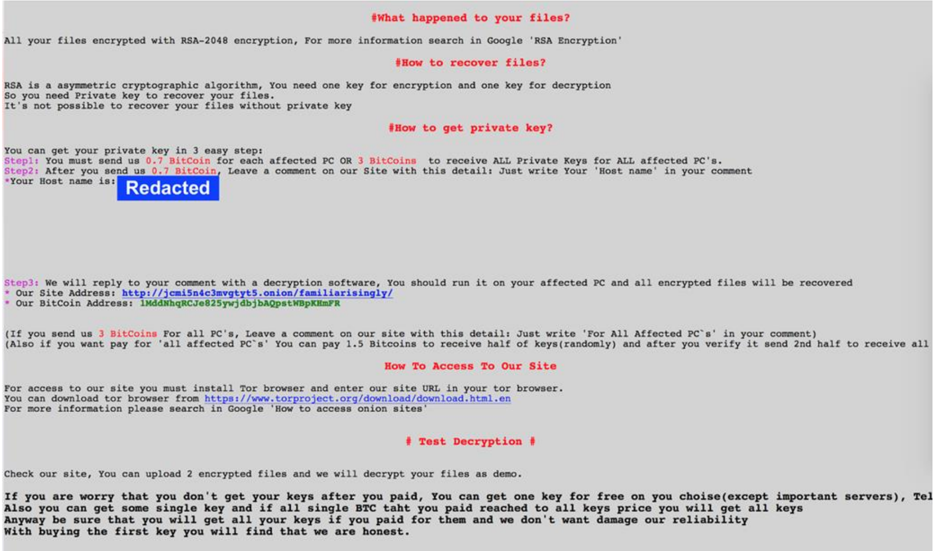
In ransomware attacks such as these, an attacker gains unauthorized access to an organization's computer network and uses ransomware software to block most or all of the organization's access to their own files and data. Access to the affected files is restricted until a ransom is paid to the attackers, and an accompanying timer usually provides only a limited amount of time to pay the ransom. The SamSam malware has been active since at least 2016 and has largely been associated with ransomware attacks in hospitals and the Healthcare and Public Health (HPH) Sector as a whole.[ii] In the recent SamSam incidents, victim organizations reported that their files were encrypted with the ".weapologize" extension and displayed a "sorry" message. This particular SamSam version has infected at least ten entities since 26 December 2017 and uses a "0000-SORRY-FOR-FILES.html" ransom note.[iii] While most of the victims in this string of SamSam attacks are from the US, there appear to be a few from Canada and India.

Beyond being a minor inconvenience, ransomware attacks can have impacts on patient care and delivery within the HPH sector. As a result of a recent attack on one hospital, an outpatient clinic and three physician offices were unable to use that hospital's network to access patient history or schedule appointments. This unavailability affected between 60 and 80 patients.[iv]

Ransomware can even impact patient care through attacks at supporting medical IT institutions. In a recent incident, an electronic practice management and health records provider for the HPH sector reported a SamSam infection in at least two of its data centers. This incident affected services to approximately 1,500 customers (medical practices), resulting in disruptions to non-critical patient care at a number of customer facilities.

## METHODOLOGY:

Per publicly available reporting by Talos, Cisco IR Services are investigating a new variant of the SamSam ransomware – also referred to as SamSa and Samas – that has been observed across multiple sectors (government, healthcare, and ICS) this year (2018). While the SamSam attacks have occurred across multiple sectors, they are not necessarily targeted and appear to be more opportunistic in nature. As in previous campaigns from this group, the attacker is believed to gain initial access to the target systems through open vulnerabilities, before gaining access to additional computers once inside the network and deploying the SamSam malware. For example, in 2016, the attackers exploited vulnerable JBoss webserver hosts to infect victims with SamSam. In one 2017 incident, attackers leveraged an unpatched vulnerability on a public-facing web server to compromise the server, get a foothold on the victim’s network, and deployed the SamSam ransomware.[v]



```
#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.7 BitCoin for each affected PC OR 3 BitCoins  to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.7 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: Redacted




Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: http://jcmi5n4c3mvgtyt5.onion/familiarisingly/
* Our BitCoin Address: 1MddNhqRCJe825ywjdbjbAQpstWBpKHmFR

(If you send us 3 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC`s' in your comment)
(Also if you want pay for 'all affected PC`s' You can pay 1.5 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'


# Test Decryption #


Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tel
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.
```

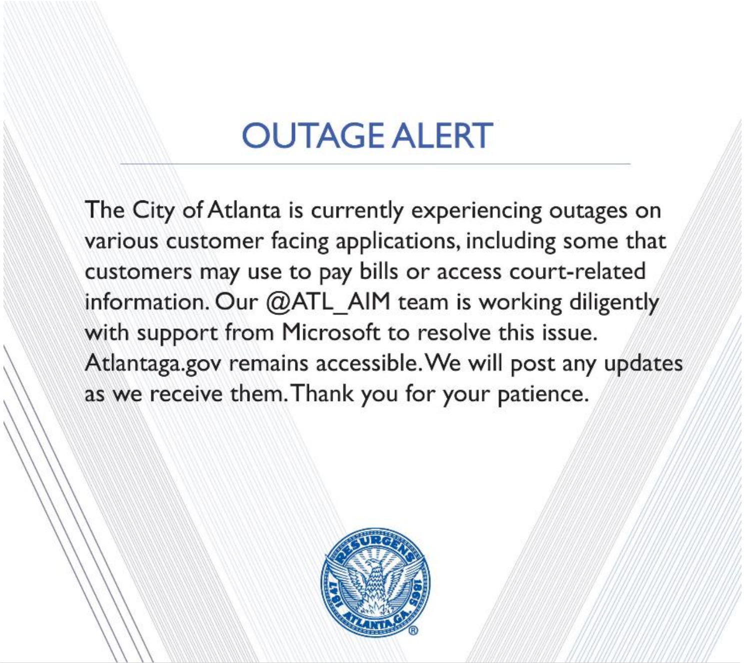
Figure 1: Ransom note displayed by the new 2018 SamSam variant, demanding a BitCoin payment and providing instructions on how to do so.

In 2018, the trend of targeting vulnerable, public-facing servers continued for the attackers behind the SamSam campaigns and, although the infection vector for the ongoing campaigns is yet to be confirmed, there has been some discussion among researchers that the attackers’ initial foothold may have been a compromised RDP/VNC servers (Remote Desktop Protocol/Virtual Network Computing). The SamSam group is reported to scan the Internet for computers with open RDP connections and then break into networks by brute-forcing the RDP endpoints. [vi]

## RECENT INCIDENTS:

### ATLANTA, GA

On 22 March 2018, the City of Atlanta held a press conference to announce a ransomware event that had resulted in a loss of access to files and outages to several of the city's online systems and services, including payment portals for city bills and access to court information. [vii] Reportedly, the attackers demanded $6,800 to decrypt each infected computer or $51,000 for the decryption keys to recover all the infected computers. Following the press conference, security researchers pointed out that certain servers belonging to the city of Atlanta had Server Message Block version 1 (SMBv1) that was internet-facing – this was the same vulnerability that enabled the EternalBlue exploit used to spread both WannaCry and NotPetya ransomwares.[viii]



OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.

Figure 2: City of Atlanta's announcement of an outage alert of customer facing applications

### COLORADO DEPARTMENT OF TRANSPORTATION (CDOT)

On both 21 February and 01 March 2018, CDOT's systems related to human resources and payroll were affected by SamSam, which had encrypted files on all employee computers running Windows OS and McAfee anti-virus software, according to an investigation.[ix] As a result, approximately 2,000 computers were pulled offline and employees were forced to use pen and paper to perform their duties.[x]

### INDIANA HOSPITAL

In another recent incident involving SamSam, on 11 January 2018, the attackers had gained access to the hospital system by using a remote-access portal, and logged in with an unnamed vendor's username and password. According to the hospital's President and CEO, the hackers utilized compromised account credentials to target a server located in the emergency IT backup facility utilized by the hospital – located many miles away from the main campus – and made use of the electronic connection between the backup site and the server farm on the hospital's main campus to deliver the SamSam payload. According to Pondurance, a forensic firm, no patient data had been compromised or exfiltrated, and the FBI confirmed that the group behind SamSam is more interested in receiving the ransom than in harvesting patient data.[xi]

**EHR PROVIDER**

On 18 January 2018, a cloud-based Electronic Health Record (EHR) provider disclosed that their Professional EHR service and their Electronic Prescription of Controlled Substances ("EPCS") service were disrupted due to ransomware events at their North Carolina data centers. Open media reporting suggested that the variant of SamSam that infected the company was a new variant unrelated to the version of SamSam that reportedly infected two hospital systems the previous week.[xii]

Media reports indicate that roughly 1,500 medical organizations using the EHR service were impacted by the attack. Customers noted on social media inabilities to login to their cloud-based accounts, while doctors tweeted they've been forced to cancel patient appointments, pay staff overtime, and had little to no access to patient records.[xiii] Additionally, HIStalk, a health IT web blog, reported that some customers have disclosed issues with other tools beyond the Professional EHR and EPCS.[xiv]

The affected tools are part of a patient engagement platform and are used to support and connect 45,000 physician practices, 180,000 physicians, 19,000 post-acute agencies, 2,500 hospitals, 100,000 electronic prescribing physicians, 40,000 in-home clinicians, and 7.2 million patients.[xv] Disruptions to these services are impacting secure patient communication with providers, electronic medical records access, and even bill payment via web portals.[xvi] The disruptions are expected to continue for the duration of the incident.

## MITIGATION STRATEGIES, CONTINGENCY & BUSINESS CONTINUITY PLANS FOR RANSOMWARE

In order to prevent attackers from gaining access to servers via RDP, as is the case with many ransomware events, the following mitigations strategies are recommended[xvii]:

- restrict access behind firewalls and by using a RDP Gateway, VPNs
- use strong/unique username and passwords with two-factor authentication (2FA)
- limit users who can log in using remote desktop
- implement an account lockout policy to help thwart brute force attacks (set a maximum number of attempts before locking out the account)

The *Contingency Planning SAFER Guide* specifically discusses how healthcare organizations can best approach planned or unplanned EHR downtimes as a result of Ransomware or hardware infrastructure failures.[xviii] According to the Office of the National Coordinator for Health

Information Technology (ONC), "effective contingency planning addresses the causes and consequences of EHR unavailability, and involves processes and preparations that can minimize the frequency and impact of such events, ensuring continuity of care."[xix]

The following practices should be considered to help ensure business and healthcare continuity in the face of potential disruptions from ransomware or other factors:[xx]

- Back up data regularly, and verify the integrity of those backups and test the restoration process to ensure it is working
- Conduct an annual penetration test and vulnerability assessment
- Secure your backups – ensure backups are not connected permanently to the computers and networks they are backing up. Examples include securing backups in the cloud or physically storing backup data offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously backup in real time, also known as persistent synchronization. Backups are critical in ransomware recovery and response; if infected, a backup may be the best way to recover critical data.

Recommendations for handling incidents involving computers infected with ransomware:[xxi]

- **Isolate the infected computer immediately:** Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- **Isolate or power-off affected devices that have not yet been completely corrupted** This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- **Immediately secure backup data or systems by taking them offline:** Ensure backups are free of malware.
- **Contact law enforcement immediately:** It is strongly encouraged to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- If available, **collect and secure** partial portions of the ransomed data that might exist.
- **If possible, change all online account passwords and network passwords after removing the system from the network:** Furthermore, change all system passwords once the malware is removed from the system.
- **Delete Registry values and files to stop the program from loading**.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification regulations require HIPAA covered entities and their business associates to safeguard protected health information (PHI). The HIPAA Security Rule requires implementation of security measures that can help entities prevent the introduction of ransomware as well as assist entities in how to respond and recover from ransomware attacks. Some of these required security measures include:[xxii]

- Conducting a risk analysis to identify and assess risks to electronic protected health information (ePHI);
- Implementing security measures to mitigate or remediate identified risks;
- Implementing procedures to guard against and detect malicious software;
- Training users to assist in detecting malicious software and how to report such detections;
- Establishing contingency plans including data backup and recovery; and
- Developing procedures for responding to security incidents such as a ransomware attack.

**There are serious risks to consider before paying the ransom:** USG does not encourage paying a ransom to criminal actors. However, after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup. Ransomware victims may also wish to consider the following factors:[xxiii]

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom.
- Some victims who paid the demand were targeted again by cyber actors.
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

## SUMMARY DISCUSSION

The attackers behind SamSam have a history of targeting both government and healthcare organizations since 2016. The attackers have remained focused on those sectors, as well as education and municipalities, likely because those systems and networks are critical and any downtime cannot and will not be tolerated, which increases the chance that the victims' will pay the ransom. In the case of the CDOT, according to the Office of Information Technology (OIT), the regularly maintained backups enabled the systems to get back online relatively quickly and did not have to pay the ransom.[xxiv]

As evidenced by recent SamSam ransomware attacks, the HPH sector continues to face challenges from ransomware attacks. These attacks have had material impacts on healthcare services to patients, both through attacks on patient care facilities themselves and through attacks on supporting organizations. Due to the sector's reliance on IT systems and the operational importance of patient data and records, the ransomware risk to the HPH sector is expected to continue for the foreseeable future. Organizations are encouraged to utilize data backups and develop contingency and business continuity plans that can ensure resilient operations in the event of a ransomware event.

*This report was prepared by the Healthcare Cybersecurity and Communications Integration Center (HCCIC) and coordinated with the HHS Computer Security Incident Response Center (CSIRC). This is a preliminary analysis of potential vulnerabilities that continue to be researched and analyzed. It is based on the latest available information as of the date at the top of the report. Readers are advised to search for the latest authoritative information and exercise professional judgment before taking actions related to these potential vulnerabilities.*

## APPENDIX: INDICATORS OF COMPROMISE (IOCs):

The following indicators of compromise can be used with enterprise antivirus systems and host intrusion prevention tools to help prevent and mitigate against the SamSam malware. These were shared by Cisco IR Services – one of the teams reportedly working the incident response for one of the referenced incidents – and made public by Talos Intelligence in a blog post on 22 January 2018.[xxv]

File name: rony45.exe
Detection Ratio: 35/68
MD5: d8469e625ae90ab64d4aef0b63f42150
SHA-1: 4a042e44f962ad03e62494e676e377710532b7e4
SHA-256: 0785bb93fdb219ea8cb1673de1166bea839da8ba6d7312284d2a08bd41e38cb9

File name: r2.exe
Detection Ratio: 39/67
MD5: f297544a20bda66ee6f98e3dc91060c6
SHA-1: 3e140a5df3161ff5d3935b1139275e07903cfff5
SHA-256: 338fdf3626aa4a48a5972f291aacf3d6172dd920fe16ac4da4dd6c5b999d2f13

File name: r2.exe
Detection Ratio: 30/65
MD5: f161be29868df913405338499a6ee675
SHA-1: 7b7318b1c25477ea5d63dc8c563cd36fdbca8055
SHA-256: 3531bb1077c64840b9c95c45d382448abffa4f386ad88e125c96a38166832252

File name: r2.exe
Detection Ratio: 30/65
MD5: e94f4ddc46ea280332b899cc747c78e1
SHA-1: d5953a42622024ee05618da645d381973c3ed5a5
SHA-256: 4856f898cd27fd2fed1ea33b4d463a6ae89a9ccee49b134ea8b5492cb447fb75

File name: runner2.exe
Detection Ratio: 20/65
MD5: d51e9eb26afb97ff2bb43cebe75210f6
SHA-1: 14dbbec0f330df10baa423ad89e92c8345e9d70a
SHA-256: 516fb821ee6c19cf2873e637c21be7603e7a39720c7d6d71a8c19d8d717a2495

File name: runner2.exe
Detection Ratio: 35/64
MD5: 92e897f476cc29a6422e64f961d78633
SHA-1: 9800593add6c6d71e23aeaeee30d58fc2debaf68
SHA-256: 72832db9b951663b8f322778440b8720ea95cde0349a1d26477edd95b3915479

File name: runner2.exe
Detection Ratio: 37/66
MD5: 7a25b0d43047552cbdad17cfb488317d
SHA-1: 22b80abde3611407effec3140bb02bfb39b2c33d
SHA-256: 754fab056e0319408227ad07670b77dde2414597ff5e154856ecae5e14415e1a

File name: robert2.exe
Detection Ratio: 32/66
MD5: a82db52bc6f1e5477eb1809cd5f23489
SHA-1: 03c21e5ad8f0f2685821f0f74799aa1cf104e443
SHA-256: 88d24b497cfeb47ec6719752f2af00c802c38e7d4b5d526311d552c6d5f4ad34

File name: r45.exe
Detection Ratio: 33/66
MD5: 58b39bb94660958b6180588109c34f51
SHA-1: 7d21c1fb16f819c7a15e7a3343efb65f7ad76d85
SHA-256: 88e344977bf6451e15fe202d65471a5f75d22370050fe6ba4dfa2c2d0fae7828

File name: r2.exe
Detection Ratio: 32/65
MD5: 739bda4212ff42999d1401624eebcce0

SHA-1: 4485004f78a68d8fccd4fc549a40dd8c76cfca14
SHA-256: 8eabfa74d88e439cfca9ccabd0ee34422892d8e58331a63bea94a7c4140cf7ab

File name: r45.exe
Detection Ratio: 36/67
MD5: 038fb413f51b0ab7eb088e0f3ea7be90
SHA-1: 5db38eeb9d3dfba2e382cccb1364ec7ce436aecf
SHA-256: 8f803b66f6c6bc4da9211a2c4c4c5b46a113201ecaf056d35cad325ec4054656

File name: r2.exe
Detection Ratio: 42/65
MD5: 24217bb462138ff00a45e66a500f9280
SHA-1: cca80f9c7be6231c28b31a244851b80a1481f476
SHA-256: dabc0f171b55f4aff88f32871374bf09da83668e1db2d2c18b0cd58ed04f0707

File name: r45.exe
Detection Ratio: 31/65
MD5: c3e8acc131a3484ffd06af189f90f92a
SHA-1: 7201b6f7dfea98172fd09d83359f262dbf2ed4bf
SHA-256: e7bebd1b1419f42293732c70095f35c8310fa3afee55f1df68d4fe6bbee5397e

## References

[i] Catalin Cimpanu, "SamSam Ransomware Hits Hospitals, City Councils, ICS Firms", The Unhived Mind News, 22 January 2018, accessed 22 January 2018; https://theunhivedmind.com/news/2018/01/22/samsam-ransomware-hits-hospitals-city-councils-ics-firms/

[ii] Chris Brook, "HEALTHCARE PROVIDERS STILL PARALYZED FOLLOWING ALLSCRIPTS RANSOMWARE ATTACK," Digital Guardian, 25 January 2018, accessed 25 January 2018; https://digitalguardian.com/blog/healthcare-providers-still-paralyzed-following-allscripts-ransomware-attack

[iii] Hannah Grover, "City of Farmington recovering after SamSam ransomware attack," Farmington Daily Times, 18 January 2018, accessed 22 January 2018; www.daily-times.com/story/news/local/farmington/2018/01/18/farmington-recovering-after-ransomware-attack/1044845001/

[iv] David Bisson, "Another Indiana Hospital Hit by Ransomware Attack," Security Boulevard, 22 January 2018, accessed 22 January 2018; https://securityboulevard.com/2018/01/another-indiana-hospital-hit-by-ransomware-attack/

[v] Kevin Townsend, "SamSam Ransomware Attacks Hit Healthcare Firms," Security Week, 22 January 2018, accessed 22 January 2018; www.securityweek.com/samsam-ransomware-attacks-hit-healthcare-firms

[vi] Vitor Ventura, "SamSam - The Evolution Continues Netting Over $325,000 in 4 Weeks," Talos Intelligence, 22 January 2018; accessed 24 January 2018; blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html

[vii] Jonathan Crowe, "City of Atlanta Hit with SamSam Ransomware: 5 Key Things to Know," Barkly, March 2018, accessed 29 March 2018; https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam

[viii] Reggie (@Ring0x0), Twitter post, 23 March 2018, accessed 29 March 2018; https://twitter.com/Ring0x0/status/977230686661894144

[ix] David Bisson, "Another Ransomware Variant Strikes Colorado DOT Days after Initial Attack," Tripwire, 02 March 2018, accessed 30 March 2018; https://www.tripwire.com/state-of-security/latest-security-news/another-ransomware-variant-strikes-colorado-dot-days-after-initial-attack/

[x] David Bisson, "Another Ransomware Variant Strikes Colorado DOT Days after Initial Attack," Tripwire, 02 March 2018, accessed 30 March 2018; https://www.tripwire.com/state-of-security/latest-security-news/another-ransomware-variant-strikes-colorado-dot-days-after-initial-attack/

[xi] Steve Long, "The Cyber Attack – From the POV of the CEO," Hancock Health, 19 January 2018, accessed 22 January 2018; https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/

[xii] Steve Ragan, "Allscripts recovering from ransomware attack that has kept key tools offline," CSO, 21 January 2018, accessed 22 January 2018; https://www.csoonline.com/article/3250246/security/allscripts-recovering-from-ransomware-attack-that-has-kept-key-tools-offline.html#tk.twt_cso

[xiii] Chris Brook, "HEALTHCARE PROVIDERS STILL PARALYZED FOLLOWING ALLSCRIPTS RANSOMWARE ATTACK," Digital Guardian, 25 January 2018, accessed 25 January 2018; https://digitalguardian.com/blog/healthcare-providers-still-paralyzed-following-allscripts-ransomware-attack

[xiv] "Ransomware Attack Takes Down Some Allscripts Systems," HIStalk, 18 January 2018, accessed 26 January 2018; histalk2.com/2018/01/18/ransomware-attack-takes-down-some-allscripts-systems/

[xv] "Allscripts by the Numbers," Allscripts, accessed 25 January 2018; www.allscripts.com/about-allscripts

[xvi] Jonah Comstock, "Allscripts taps Vidyo to integrate telehealth into its patient portal," Mobi Health News, 30 August 2017, accessed 25 January 2018; www.mobihealthnews.com/content/allscripts-taps-vidyo-integrate-telehealth-its-patient-portal

[xvii] Jonathan Crowe, "City of Atlanta Hit with SamSam Ransomware: 5 Key Things to Know," Barkly, March 2018, accessed 29 March 2018; https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam

[xviii] Elizabeth Snell, "Ransomware Attack Mitigation in Updated ONC SAFER Guide," Health IT Security, 24 March 2017, accessed 26 January 2018; https://healthitsecurity.com/news/ransomware-attack-mitigation-in-updated-onc-safer-guide

[xix] "Contingency Planning," Health IT, accessed 26 January 2018; https://www.healthit.gov/safer/guide/sg003

[xx] "Ransomware Prevention and Response for CISOs," FBI, accessed 26 January 2018; https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[xxi] "Ransomware Prevention and Response for CISOs," FBI, accessed 26 January 2018; https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[xxii] “Fact Sheet: Ransomware and HIPAA,” HHS Office for Civil Rights, accessed 5 April 2018; https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

[xxiii] "Ransomware Prevention and Response for CISOs," FBI, accessed 26 January 2018; https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[xxiv] Uzair Amir, "2,000 Colorado DOT computers infected with SamSam Ransomware," HackRead, 23 February 2018, accessed 30 March 2018; https://www.hackread.com/2000-colorado-dot-computers-with-samsam-ransomware/

[xxv] Vitor Ventura, "SamSam - The Evolution Continues Netting Over $325,000 in 4 Weeks," Talos Intelligence, 22 January 2018; accessed 24 January 2018; blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html