CSO
FROM IDG
BUSINESS RISK LEADERSHIP

INSIDER EXCLUSIVE

# ALLSCRIPTS:
## Ransomware, recovery, and frustrated customers



*The actors behind **SamSam launched an attack against Allscripts** in January 2018, leaving the company's customers without access to the services needed to run their medical practices – some for more than a week. **Here's what happened and where things went wrong.*** **BY STEVE RAGAN**

GETTY IMAGES

## RANSOMWARE, HEALTHCARE AND INCIDENT RESPONSE:

# Lessons from the Allscripts attack

*The actors behind SamSam launched a **devastating attack** against Allscripts in January, 2018. As Allscripts worked its incident response plan, **things started to unravel.** Here are the lessons learned.*

**ON JANUARY 18, 2018,** at around 2:00 a.m. EST, the security operations center (SOC) at electronic health record (EHR) and practice management software provider Allscripts detected abnormal activity.

Four hours later, at 6:00 a.m. EST, the SOC started their investigation and determined the abnormal activity was in fact a full-blown ransomware incident due to SamSam, a family of ransomware that is known to target healthcare organizations. A short time later, teams from Microsoft, Mandiant and Cisco were called in to help.

At this point, as is the case for any organization facing a large-scale incident, Allscripts said the situation turned into a "crisis event." It was quickly determined that the Professional EHR (Pro EHR) and Electronic Prescriptions for Controlled Substances (EPCS) services were the hardest hit. Allscripts told Salted Hash in a statement that approximately 1,500 medical practices were impacted by the incident.

Incident response is something that most IT and security professionals are drilled on. It's a process that sometimes requires a specific mindset to deal with stressful situations; and a process with challenges that are unique to each business.

We examine the recent SamSam ransomware attack at Allscripts, following the phases of incident response as documented by SANS.

## Preparation

As the heading suggests, the first step in building out an incident response plan is preparation. Incident response teams have to prepare as best as they can for a number of incidents, from power outages, hardware failures and malware to tornados, floods and earthquakes — and everything in between.

By all accounts Allscripts did this, and in a statement the company told Salted Hash that they "prepare and drill" for various possible incidents ahead of time. In addition, the company conducts regular blue team and red team exercises.

However, it isn't clear to what extent ransomware was part of their drills, as the company didn't offer any insight into its incident response program or the mindset


## Allscripts recovery

The ransomware attack against Allscripts had serious consequences for its customers. Here is a timeline from detection until the last notice by the company.

**JANUARY 18**

**2:00 a.m.** EST

**Allscripts detects something unusual in its network.** Incident response teams begin investigating.

**6:00 a.m.** EST

Allscripts incident response determines that **SamSam, a family of ransomware, is responsible for the anomaly.** Systems have been infected (encrypted) and as a result data centers in Raleigh, NC and Charlotte, NC are taken offline. Professional EHR and EPCS are the hardest hit applications. **Customers lose access to their accounts.** Sometime later that day, teams from Microsoft, Mandiant and Cisco are called in.

behind its development when asked about it.

Based on comments made to the public by Allscripts, posts to the Allscripts ClientConnect portal by customers and company representatives, status update calls during the incident, and conversations with customers, Salted Hash is confident that Allscripts had an incident response plan in place (as they should), but there were some snags once the plans were actually put to the test during a real-world incident.

The SamSam ransomware attack against Allscripts started on a Thursday, and most customers reported they were offline or continued to have access problems until Thursday the following week.

> With the threat identified and containment achieved, **Allscripts had to turn its focus to eradication and recovery.**

For example, after Allscripts reported that systems for Allscripts Practice Management (PM) and Pro EHR "were restored in the East, Central, Mountain, and Pacific regions" on Tuesday, January 23, many clients in those areas reported zero access.

"We are currently working to restore permissions for all users. Once permissions are restored, users will have access to their core applications. We are continuing to work on restoration of interfaces," an Allscripts update note explained.

So, while customers could access the cloud — as one customer observed — most couldn't actually access the database. This was a key problem for many of the customers impacted by the attack, as they're hosted customers. All of their practice information lives in the cloud, from patient records to billing details, lab results and more.

A number of customers turned to the ClientConnect forum to vent their frustrations in response to daily updates:

"A lot of talking but not really saying anything," one customer wrote early on Tuesday morning.

"I am not restored yet despite the promise yesterday of 18- 24-hour restoration. Who cares if you can access the cloud if that just takes you to a dead site? It has been 6 days people, I do not want to hear that you are diligently working on it around the clock. I want results not mumbo jumbo."

Salted Hash asked Allscripts about the disconnect between the status update and the reality for customers, such as why customers were still having issues even after the company said systems were restored.

"Allscripts serves a wide range of clients in a variety of individual circumstances. Accordingly, they experienced different effects as a result of this incident," the company

## TIMELINE (CONT.)

### JANUARY 19

**1:00 p.m.** CDT

Allscripts issues an update that **four services are restored.**

**4:30 p.m.** CDT

Allscripts issues another update, adding **fifteen more restored services** to the list.

**8:00 p.m.** CDT

Allscripts reports progress in restoring services. **The Pro EHR service is still down.** Customers report problems accessing services.

### JANUARY 20

**9:00 a.m.** CDT

**Allscripts posts a brief update stating that they are working to bring services back online.** Customers flood the ClientConnect forum with complaints and worries about data compromise.

**2:30 p.m.** CDT

The company updates customers on the list of services that have been restored. **However, access remains a problem, and customers are vocal about it.** Pro EHR service is still down.

**10:00 p.m.** CDT

Allscripts says their first hosted Pro EHR and PM client is back online. **Customers point out the normal route a hosted customer would take to access services is still offline**, questioning how this client was able to access their data. Allscripts promises to work "though the night" to restore services.

### JANUARY 21

**11:00 a.m.** EST

Allscripts says that "careful recovery" of Pro Suite and Allscripts PM continues, but also shares news that most customers have been dreading. **The outage that started the previous Thursday will not be resolved by start-of-business on Monday.**

said. "There were a range of circumstances involved with getting particular systems back online and we addressed each of them as quickly as possible."

## Identification and containment

Allscripts identified the problem, meeting the requirements of the identification phase, when they determined the detected issues were ransomware related and furthered this identification by confirming the ransomware was SamSam, a family of ransomware known for targeting healthcare organizations.

In order to limit damage and prevent further damage, as required by the containment phase, Allscripts started severing connections with their data centers in Raleigh and Charlotte, N.C. No business wants to cut its own backbone, but sometimes the hard calls have to be made.

As mentioned, Allscripts detected something strange at around 2:00 a.m. EST on January 18, and by 6:00 a.m. EST had determined that it was a full-blown ransomware incident, requiring the assistance of teams from Cisco, Mandiant and Microsoft.

In a statement, Allscripts said that hundreds of personnel worked on the response, calling the first 24-hours an "intense swirl of many technical, business, and other practical challenges."

Allscripts stated that they drill for various security incidents, and when asked, confirmed they participate in data sharing programs with other medical organizations.

In a statement, the company said they have data sharing relationships with the FBI, the North Carolina Healthcare Information & Communications Alliance, Inc. (NCHICA), and a group of healthcare industry CISOs. They also use outside advisors who "serve as additional eyes and ears."

When asked how prepared they were for the eventuality of a ransomware attack, especially since SamSam had previously been used against two other healthcare organizations, Allscripts responded: "Keep in mind that there were no antivirus signatures available for this SamSam variant at the time it struck Allscripts. This was an entirely new, zero-day variant of SamSam ransomware that had never been identified previously by Cisco, Microsoft

## TIMELINE (CONT.)

### JANUARY 21

**4:00 p.m.** EST

Allscripts says the company will **"continue to execute on the careful recovery of the hosted national Pro Suite and Allscripts PM environment with resources committed around the clock to restoring service."**

### JANUARY 22

**12:00 a.m.** EST

Allscripts repeats the warning that they cannot promise services will be restored by Monday. **The company says that service will be restored on a rolling basis, and customers will be contacted once that happens.** Angry customers vent their frustrations in the ClientConnect forums.

### JANUARY 23

**9:30 a.m.** EST

Allscripts says they are **"making material progress."** At this time the company also says that services have been restored in the East, Central, Mountain, and Pacific regions. **The company discusses permissions issues and promises to address them.** Customers immediately respond with details of how they're in the areas listed as restored yet have no access to their data.

## SamSam's reach extends beyond healthcare

**While SamSam has been** disproportionately used against healthcare organizations since it arrived in the public view in 2016, not all of its victims are medical.

In February (a few weeks after the Allscripts attack) the Colorado Department of Transportation's (CDOT) network was infected with a variant of SamSam, impacting about 2,000 employees and leading to a number of logistical problems.

A week later, while still recovering from the first attack, CDOT was infected with a second variant of SamSam. Two attacks within two weeks. And while endpoint defenses were patched to prevent further spread (CDOT uses McAfee), the damage was already done. ◆

or the FBI. We were able to contain it within minutes, and then begin the intense work of restoring those client services that were affected."

## Defending against SamSam

By their own account Allscripts has access to a large pool of threat intelligence and information sharing. Cisco is one of their vendors, and their threat intelligence teams have done extensive work on SamSam.

Threat intelligence sources within the healthcare industry have known for some time that the group behind SamSam constantly makes modifications (variants) to the ransomware's code in order to alter how it loads on a victim's machine, thus bypassing antivirus and other endpoint defenses.

Moreover, those same sources also know that the actors behind SamSam don't rely on spam-like delivery tactics to infect victims, opting instead to infect individual systems and manually deploy the ransomware.

As such, the threat intelligence sources who spoke to Salted Hash say the key to defending against SamSam, something that would be central to any threat model and corresponding threat map, is the realization that signatures and endpoint defenses alone are not enough.

Instead, the key to stopping SamSam is a mix of endpoint defenses, patch management, limiting system functionality (disable everything that isn't needed for the system to perform its core role or function), and limiting user permissions.

Was Allscripts aware of this? Salted Hash asked Allscripts a number of SamSam-related questions in order to determine where the information gaps were and how up-to-date their systems were, but the company declined to answer any of them. Instead Allscripts simply stated, "this was a new ransomware variant for which no antivirus or patch was available."

It's important to note, though, that each organization is different, so achieving harmony between endpoint defenses, system functionality, user permissions and patch management isn't as easy as it sounds when dealing with large enterprise operations.

SamSam isn't a case of "if you only

> At this stage it's **critical** that Allscripts **understand** how the attack happened and take steps to ensure it can't happen again, such as **patching** vulnerable systems or **resetting** compromised passwords.

## TIMELINE (CONT.)

### JANUARY 24

**6:00 a.m.** EST

Allscripts says that **access to Pro EHR and PM is "now available to nearly all clients"** They warn that users may experience slowness when accessing or using their services. The company pushes the Pro Mobile solution for access, but customers are not happy with this offering. **Customers still report access problems.**

**11:30 a.m.** EST

**Allscripts repeats their claims** from 6:00 a.m. EST concerning access to Pro EHR and PM. **One customer calls the claims of access a lie**, and other customers log complaints of being unable to access any of their records.

**5:00 p.m.** EST

**Allscripts reports that 9,200 users are logged into the Pro EHR;** customers continue to report access problems. The company encourages the usage of Pro Mobile, **but the service is only available for users on iOS platforms.** Those using it say it is no solution, as it doesn't offer the feature they're expecting for office management and patient care.

### JANUARY 25

**10:00 a.m.** EST

**Allscripts reports that access to hosted Pro EHR and PM is now available to customers via desktop and mobile offerings;** they say they are aware of access issues and that they're working with Microsoft to address the issues. Customers continue to report access problems.

### JANUARY 29

Customers move to discussing a letter from Allscripts' CEO about the incident in which he promises a 33% reduction to hosted customer invoices. **Not all customers affected by the outage got this letter,** according to comments on ClientConnect. Most report restored services, but **some say sporadic connection issues remain.** ◆

do this, you'll be fine" or "work this checkbox magic here please."

Dealing with threats like SamSam requires effort and a lot of bridge building because multiple units within the organization have to come together in order to develop a workable solution.

## Eradication and recovery

With the threat identified and containment achieved, Allscripts had to turn its focus to eradication and recovery. This is where most of the pain lives for any organization dealing with an incident, as speed is the goal, but that isn't always possible when critical systems are involved. You have to clean and restore systems and then test them before putting them back into production. It's a daunting task at times.

At this stage it's critical that Allscripts understand how the attack happened and take steps to ensure it can't happen again, such as patching vulnerable systems or resetting compromised passwords — two things the actors behind SamSam often leverage in an attack.

It isn't clear what happened during this phase, though, as Allscripts has declined to discuss it.

Allscripts moved quickly to restore systems, reporting that more than a dozen services already were or would be up and running by January 19. Each day, sometimes more than once a day, Allscripts updated customers on the recovery efforts and added new services to the list of those restored.

On January 26, in a letter to customers, Allscripts CEO Paul Blade said that the company would be accelerating their plans to replicate Professional EHR across multiple data centers and a technology refresh "to shorten our recovery time in the event of any future disruption."

When asked about the data replication and the use of virtualization, Allscripts told Salted Hash that they use virtualization when it's reasonable and appropriate but added that they didn't attempt to spin up any of their replication servers to help with the restoration process.

While the incident response plan developed by Allscripts worked (after all they were able to recover from the SamSam attack), there was still a good deal of pain during this process for their customers.

## Lessons learned

Often during the containment phase an organization needs to do some sort of public contact with partners and customers, perhaps even with industry peers or regulatory bodies. But for Allscripts, the communication was a pain point.

Updates and answers from support representatives posted in the ClientConnect forum conflicted with reports from customers.

For example, customers were told on ClientConnect that the EPCS application, called ePrescribe, was online. That same day, customers reported intermittent access or lock-ups once the output icon was clicked. When a support ticket was filed, the customer was told it was a known issue related to the ransomware and that the company was working on it.

This frustrated customers, who perceived that Allscripts wasn't being truthful. But Allscripts was being truthful; the services were up, the problem was access. So, the internal definition of up or online and what the customer is expecting those terms to mean just wasn't jiving.

Customers, for the most part, are forgiving — if you're open and communicative. The key, though, is to communicate in a way they understand.

Tech professionals could make the argument that Allscripts did restore services and the systems were online within 24 hours, but the reality is that customers were down or experienced intermittent issues for at least six days and longer in some cases. These may be outlier cases, but as long as they exist, the incident isn't resolved. ◆

*–Steve Ragan*

> Dealing with threats like SamSam **requires effort and a lot of bridge building** because multiple units within the organization have to come together in order to develop a workable solution.

# Customers describe the impact of the Allscripts ransomware attack

***There were three victims during the SamSam ransomware attack*** – *the company, its customers, and the patients those customers serve.*

**A RANSOMWARE ATTACK AGAINST** a SaaS provider hurts customers, but when it's a healthcare company that's hit, patients suffer. Such was the case with January's attack against Allscripts, one of the largest electronic health record and practice management technology vendors.

By all accounts, Allscripts did a lot right. They had an incident response plan in place. They got outside help. They recovered their systems. They communicated with customers.

But as our reporting found, there was a communication gap.

When Allscripts reported a restoration to a given application or service, customers immediately reported the opposite. The root of the problem appears to be that while services were restored, access was a different matter entirely. While Allscripts acknowledged the access issues in support tickets and in some customer communications, the message being conveyed sounded like misdirection to some customers. But that wasn't Allscripts' intent at all (far from it), which is why communication during an incident is so vital.

## Crisis communications

The key to communication is to explain things in a such way that the intent of the message and its objectives are clear. To put it another way, you need to speak on your customers' level.

Crisis communications is an important aspect of incident response when the organization experiencing the incident needs to communicate with partners, regulatory bodies, or its customers. It's also a good idea to have one channel of communications, a single voice, in order to prevent conflicting statements.

In Allscripts' case, when the company reported that systems were brought back online January 23 (five days after the incident started), customers rejected that notion because they couldn't access the tools and services needed to do their jobs. Allscripts certainly brought those services back online, but the actions didn't meet customer expectations. To Allscripts' customers, online meant that things were back to normal, as if the ransomware attack never happened, which wasn't the case.

## Impact at scale

Allscripts was victimized by the actors behind the SamSam family of ransomware on Thursday, January 18. While the company was able to activate its incident response plan and restore some services within hours, many customers were

without access until the following Thursday.

The company said their Professional EHR and Electronic Prescriptions for Controlled Substances (EPCS) services were the hardest hit by the ransomware attack. In addition, customers also reported issues with Allscripts Practice Management (PM), and other tools within the suite.

Customer quotes from Allscripts ClientConnect portal

Allscripts says that about 1,500 medical practices were impacted by the ransomware attack. It's likely that this figure represents the number of practices hosted in the Raleigh and Charlotte data centers, which were disconnected during the incident.

However, any organization operating in the healthcare space should realize that 1,500 practices could represent hundreds of doctors and other medical practitioners, as well as thousands of patients. On its website, Allscripts claims a "client base of 180,000 physicians across approximately 45,000 ambulatory facilities, 2,500 hospitals and 17,000 post-acute organizations."

What follows is a look at the pain experienced by the secondary victims of the SamSam attacks against Allscripts, that is, the medical practitioners and their staffs. These accounts illustrate the real-world impact of such attacks. We are publishing them in order to stress the need to properly prepare for the eventuality of a devastating attack, as well to show how widespread and serious the impact could be.

***Our patient care is suffering!*** *We are an OB/GYN office - How many days of your doctor not being able to access your records during pregnancy is ok for you?*

***It's totally embarrassing*** *when a patient says this never happens at my other doctor's offices, and they have electronic medical records.*

***This is major.*** *Patient safety is our biggest concern right now. We have critical lab results that need to be reviewed!*

## Customer communications

On January 23, five days after the incident started, Allscripts told customers via the ClientConnect portal that they were making "material progress" in restoring affected services:

"Since our last update, Allscripts PM and Professional EHR systems in the East, Central, Mountain, and Pacific regions have been brought back online. We are currently working to restore permissions for all users. Once permissions are restored, users will have access to their core applications. We are continuing to work on restoration of interfaces."

Immediately, customers began questioning the update, asking for ETAs and clarification concerning the wording of the message. "What does this really mean," one customer asked, "when will we [be] able to access 'core applications'?"

In response to that question another customer stated: "It means you can access the cloud but you cannot access the database yet. That is not really restored then."

Other customers chimed in, calling the update misleading: "Stop misleading your clients and give them credible facts. Either we are up or we are not. The updates from you remain the same only worded differently."

On January 24, six days after the incident started, Allscripts announced that access to hosted Pro EHR and PM was now available to "nearly all clients both through the desktop application and the Pro Mobile solution."

At the same time, customers were having problems with the mobile offering (those that could use it, as it was only available for customers on iPads and iPhones) not meeting their needs. Moreover, the messaging from Allscripts was once again causing problems.

Customer quotes from Allscripts ClientConnect portal

"We need access to PM in order to bill anything," one customer said, venting frustration. "Your mobile solution is no solution at all. What good does that do? It does not function like the actual EMR...You are hurting this practice financially, not to mention how our patients feel right now. We are not able to bill anything, post payments, run statements, etc."

Another customer, responding to a phone call from an Allscripts representative, advising them that "there have been some outages" simply had to laugh in the face of frustration.

"We have been down a week at this point and they JUST call to say SOME OUTAGES?! This is the FIRST phone call we received in a week from them! 3 or 4 employees can get in here and that is out of about 30 people. Our patient care is suffering," the customer continued.

"We are an OB/GYN office — How many days of your doctor not being able to access your records during pregnancy is ok for you? How long do you trust them when they can't help you with darn near anything? We are starting to look incompetent and Allscripts is to blame!"

Salted Hash asked Allscripts about the problems customers were experiencing, even after announcements were made that services were restored. "Allscripts serves a wide range of clients in a variety of individual circumstances. Accordingly, they experienced different effects as a result of this incident," the company said.

"There were a range of circumstances involved with getting particular systems back online and we addressed each of them as quickly as possible."

*When presented with the option of the cloud we were told that we would be more secure and protected from these types of threats. They have not held up that promise.* ***We are on day 5 of no service.***

*This has not only affected business operations, but most importantly* ***it forces my practice to provide sub-par patient care.***

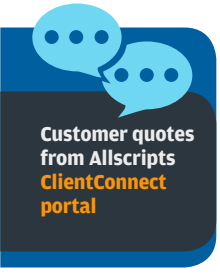
***I used to think it might be advantageous to have everything on one system,*** *but after this week, I'm so happy we had a separate EHR that we could at least still see people.*

## Everyone's eggs in one basket

It's a painful reality. A core vendor is taken offline after a serious incident, leaving the medical practitioners and their patients between a rock and a hard place. Most of Allscripts' customers selected the hosted option (going paperless) because it was economical.

"The issue is that a lot of pressure has been put on practices all over to make the move to hosted solutions and it seems great, but this very risk is almost always overlooked," one customer said, speaking to the pain experienced in the days after SamSam was first detected.

> ***I am personally fed up with the lack of meaningful communication*** *by Allscripts, their lack of any business continuity plans, and generally speaking poor services.*




And yet, even when such a risk is understood, the customer expectation is that the vendor responsible for the hosted environment will protect them from such problems. Strictly speaking, Allscripts did this, but the customers certainly didn't feel as if that were the case.

Before moving to hosted EHR/EMR solutions (or really any hosted solutions), it's important to ask the vendor (such as Allscripts) to discuss their business continuity and disaster recovery plans — specifically how they plan to respond to threats like ransomware or hardware failure, and how quickly they can get your office back up and running.

One Allscripts customer said they requested a business continuity plan from the company months before the SamSam attack. Nothing ever came of that request.

Vendors aside, it's also important for the practice to consider internal business continuity plans. One practice manager (and Allscripts customer) shared their office's process for keeping their business moving during the Allscripts outage:

"We have copies of the forms we used before going to EHR years ago. Since there are frequent outages with Allscripts we immediately convert to paper and keep on moving forward. This time I created an appointment schedule on Excel and we manually put in several days of the schedule from the Mobile App and everyone has access to the Excel spreadsheet to see who is coming in and to add appointments."

> ***We are a billing service.*** *What do we tell our client physicians when their cash flow dries up in 2-3 weeks?* ***We are at risk of losing clients.***

Unfortunately, as others pointed out, the process defeats the whole reason many moved to hosted EHR/EMR to begin with. Not to mention this process duplicates their workflow.

This particular customer said they would scan the paper chart note into the system and be done with it. It isn't pretty, but it works, and that's what counts.

## Moving forward

A letter to customers from Allscripts CEO Paul Black, dated January 26, said the company would be accelerating their plans to replicate Professional EHR across multiple data centers. This is good, because often cloud providers use multiple storage area networks (SANs) and virtual environments to speed up recovery in the event of an outage. It's certainly advisable to inquire about such features when considering hosted solutions.

However, the letter's remarks were also confusing and a bit disappointing. Specifically, the CEO's letter said that Pro EHR would be replicated across multiple data centers and that the company would perform a technology refresh to shorten recovery time in the event of future disruptions. The initial efforts are expected to be completed by September 2018. Why will it take so long? Why wasn't this done sooner? Allscripts would not answer those questions.

When asked about the data replication and their use of virtualization, Allscripts told Salted Hash that they use virtualization when it's reasonable and appropriate but didn't get into specifics.

As such, it isn't clear if their VM usage hurt or helped during the recovery process. However, given the issues and the length of the outage experienced by their customers, it's unlikely the VMs played any valuable role. The company's statement also said they didn't attempt to spin up any of their replication servers during the recovery phase. ◆

*–Steve Ragan*

# SamSam explained: Everything you need to know about this opportunistic group of threat actors

*The group behind the SamSam family of ransomware is* ***known for recent attacks on healthcare organizations,*** *but that's not its only target.*

### WHAT IS SAMSAM?

The first version of the SamSam (a.k.a. Samas or SamsamCrypt) ransomware was developed and released in late 2015 by a group of threat actors believed to reside in Eastern Europe.

The group itself is mostly a mystery, but the code it developed and the resulting pain from its usage isn't. SamSam is a serious threat to organizations of all sizes, and we've seen a spike in SamSam-related attacks this year.

Here's a breakdown of the malware itself and the group using it.

## SamSam vs. other ransomware families

Most turnkey ransomware crews or authors don't really know who they're targeting. They spread their payloads (Locky, Cerber, Dharma, Spora) via drive-by downloads, direct downloads, or malicious emails, and if there's a successful infection, they'll ask for a fee to decrypt files, say $500-$1,000 in Bitcoin (BTC).

It's a numbers game for these criminals. Infect enough people and eventually someone will pay. Usually, one or two payments is enough to cover the entire cost of the campaign; the rest is pure profit.

As Salted Hash previously reported, some ransomware authors and sellers are clearing upwards of $100,000 a year. But the SaaS model of ransomware is a cutthroat business, so most of the players in that game aren't making much from their efforts. The real money is in customization and private ransomware development. This is where SamSam stands out form the rest.

The group behind SamSam is focused, which makes its brand of extortion more lethal on the network. SamSam isn't commodity ransomware. You can't find it on a criminal forum, and it isn't sold as a service. It's developed privately and updated frequently, in order to avoid antivirus detection and other endpoint defenses. This is why most victims are discouraged when they are infected, as none of their usual endpoint defenses are able to stop it.

It should come as no surprise if proof emerges that the group behind SamSam monitors the web for mentions of their work, because as soon as one attack hits the press or security vendors publish a report (or update signatures) a new build of SamSam hits the streets.

Lately the group has targeted healthcare organizations, but they've also targeted governments, schools, and private businesses. In February, the Colorado Department of Transportation was infected twice in two weeks by SamSam, creating an administrative nightmare for the agency.

> **It's a numbers game for these criminals.** Infect enough people and eventually someone will pay. **Usually, one or two payments is enough to cover the entire cost of the campaign; the rest is pure profit.**

## An opportunistic approach to infection

"We see this group more as an opportunistic attack vector," explained Jeremy Koppen, principal consultant at Mandiant, a FireEye company.

When it comes to SamSam, opportunity doesn't knock, it scans and exploits.

Once they have a foothold on a system, the group will compromise a network and elevate privileges. The vulnerabilities targeted will depend on the victim, but if there is an exposed server or asset that's vulnerable, they'll hit it.

In 2015 and 2016, the compromise usually started with JBoss vulnerabilities. However, the group also targeted Microsoft's IIS, FTP vulnerabilities, and RDP (Remote Desktop Protocol) instances exposed to the public. Lately, the group has started to focus on single-factor external access such as RDP or VPN.

In the most recent string of healthcare attacks from the SamSam group — including Hancock Health and Allscripts — RDP was singled out as the likely point of entry onto the network.

In a statement, Hancock Health confirmed RDP as the initial point of entry. An administrative account created by a Hancock Health vendor was compromised by the SamSam group, which enabled it to pivot into the hospital's information systems.

When asked, Allscripts would not discuss how the SamSam group gained access to its environment. However, Allscripts customers use RDP to access services, and the company has login portals publicly exposed to the internet. Given the SamSam group's recent obsession with RDP, this is likely the avenue of attack.

## Compromising the network

Early on, the SamSam group used JexBoss (an open source JBoss exploitation tool). In fact, they'll still use it if needed, but recent investigations have observed a wide range of applications used to compromise and conduct reconnaissance on a victim's network.

# They'll fight back

**SECUREWORKS NOTED** an interesting evasion technique used by the SamSam group in 2017. When Mimikatz was detected by the victim's endpoint protection, the group modified a registry entry to disable the endpoint tool's scanning. This changed enabled them to use Mimikatz as normal and collect credentials for two dozen user accounts.

These observations confirm that SamSam attacks are manual, so someone is sitting behind a keyboard.

According to forensic experts who have worked cases involving SamSam, the group will use any or all of the following tools:

- **Mimikatz** - A tool to extract passwords, hash, PINs, and Kerberos tickets from memory
- **reGeorg** - A reverse proxy / web shell script
- **PsExec** - Used to launch interactive command prompts on remote systems
- **PsInfo** - Used to gather information about local or remote systems
- **PaExec** - An alternate, redistributable version of PsExec
- **RDPWrap** - Allows console and remote RDP sessions at the same time
- **NLBrute** - An exploit tool for public-facing RDP instances
- **Impacket** - A collection of Python classes that enable security teams to work with network protocols. (SamSam was observed using wmiexec.py in January of 2017.)
- **CSVDE** - An Active Directory tool, ships with Windows Server. Used to import or export entries from Lightweight Directory Access Protocol (LDAP); Active Directory; Active Directory Application Mode (ADAM); Active Directory Lightweight Directory Services (ADLDS); and Active Directory Domain Services (ADDS)
- **PowerSploit** - A collection of PowerShell scripts used for reconnaissance and persistence

The reconnaissance phase also includes testing to ensure control. One investigator discovered that a simple file — text.txt — was written on systems throughout the victim's environment. ◆

## Pay up, or hope your backups work

Once the network is compromised, the SamSam group will launch the ransomware. Just before that happens though, the group will determine a ransom price that's commensurate with the level and volume of data they're going to encrypt and the victim's ability to pay.

A victim who doesn't appear to be able to pay high amounts will be presented with a smaller ransom. But a large company, such as Allscripts, will need to pay considerably more.

"Originally, we saw a group that charged roughly 1 BTC per infected system, but that's also back in that late 2015 time period, where Bitcoin was obviously less valuable. I think recently, we've seen about 0.7 BTC [per system], so it's dropped a little bit, and a higher Bitcoin value to decrypt all systems. A recent one we saw was 3 BTC to decrypt all systems," Koppen said.

By pricing the ransom at an affordable level (as well as targeting critical systems and forcing a halt to operations), the SamSam group is encouraging payment, especially if the cost of recovery is higher than the ransom.

This is exactly what happened with Hancock Health in Greenfield, Indiana. When the hospital was infected with SamSam earlier this year, they opted to pay the ransom demand in order to restore operations quickly.

## Market moves

The constant flux in the Bitcoin market has an impact on the profit margins for criminals pushing ransomware, even the SamSam group. One of the SamSam group's Bitcoin wallets, where Hancock Health sent its ransom payments, collected 30.4 Bitcoins between December 25, 2017 and January 20, 2018.

**A victim who doesn't appear to be able to pay high amounts will be presented with a smaller ransom.** But a large company, such as Allscripts, will need to pay considerably more.

At the time of the last transaction, the Bitcoins were worth $392,291.02. However, based on the exchange rate at the time this article was drafted (March 14, 2018) the coins are only worth $264,257.47, a loss of $128,033.55.

This assumes the group didn't cash out in January when the exchange rate was higher. The opposite effect is true as well, as the coins could increase in value over time.

Examining one of the Bitcoin wallets used by the SamSam group and comparing the transaction data to the public reports of Hancock Health's payment, you can see the hospital's record.

Hancock Health paid the ransom at 2:31 a.m. on Saturday, January 13, 2018; within two hours its systems were restored. In all, it paid 4 BTC, or $56,707.40, based on the price of Bitcoin at the time. News reports pegged the payment at $55,000 even.

In an interview with local media, Hancock CEO Steve Long said those responsible for infecting his network made it easy to pay, adding "they price it right."

The SamSam group's wallet also shows two other payments, one for 4 BTC and another for 5 BTC, made on January 19, 2018.

This is around the time Allscripts was recovering from its attack.

Did Allscripts pay the ransom in order to speed up the recovery effort?

Salted Hash asked the company for details, but Allscripts declined to answer. In a statement, a company spokesman cited security reasons and said, "we cannot provide additional information about our specific recovery efforts."

If the company did pay, it isn't clear if the payment helped at all. As previously reported, some Allscripts customers were without access for at least a week in most cases, longer in others. If the payments are unrelated to Allscripts, then there are two additional SamSam victims in Q1 2018 that the public doesn't know about.

## Stopping SamSam and others like it

If the SamSam crew is successful in its efforts to encrypt your systems, your problems started long before any ransomware infection. As mentioned, the crew behind SamSam is opportunistic when it comes to

victims, looking for easily exploited systems and services. Once it finds them, the clock starts ticking.

It isn't an easy task to stop dedicated attackers like the SamSam group, and while the processes below will certainly help, they'll require a certain amount of dedication on your part. For groups like this, a "set it and forget it" mentality simply will not do.

**Detection:** The first step, according to many incident response professionals Salted Hash spoke with is detection. It isn't easy, but the quicker you can detect a problem and react to it, the better off you are. It took Allscripts four hours to detect SamSam and declare a ransomware event and start the incident response process. Can you do it faster?

Being able to spot anomalies like the use of common administration tools like PsExec by users who have no reason to use such things will aid in quicker detection. The challenge, though, with anomalous behavior detection is the fact that the SamSam group will often use whitelisted tools and valid credentials in order to avoid tripping any alarms.

**Patch management:** Exploiting vulnerabilities in FTP software, Microsoft's IIS, Windows Server, JBoss and more, the SamSam crew has proven it isn't too picky when it comes to the initial point of entry. Having a solid patch management program and working towards shortening the time between a patch's release and its deployment into the production environment will go a long way towards hurting the SamSam crew's efforts.

**AV and other endpoint protections:** Don't ignore endpoint defenses; they're still a vital layer to your organization's overall security posture. But at the same time, don't count on them to consistently stop groups like SamSam. As mentioned, the group behind SamSam constantly updates its ransomware to avoid endpoint defenses. The group also takes the necessary steps to circumvent those defenses during the network compromise or reconnaissance phase of the attack.

**Least privilege:** This is key. Keeping users on the least privileged level for their account not only limits the hijinks the SamSam crew will get up to, but helps lower the impact for almost any other attack against the organization. If a user requires administrator access, it should be stressed that it only be used as needed, and such access should always be monitored.

**Authentication:** Using multifactor authentication, particularly for VPN and remote services, is key. Single-factor authentication paths have been hard hit by the SamSam crew, but aside from the risk on that front, using multiple layers of authentication just makes sense and should be encouraged when possible.

**Access controls:** The Department of Justice, in their guidance on ransomware, stresses configuring access controls with least privilege in mind. Such controls include file, directory, and network share permissions, with a focus on restricting write access to identified files, directories, and shares.

Likewise, implementing Software Restriction Policies to prevent execution in temporary folders is also a smart move. Whitelisting, too, is a strong recommendation.

**Limited functionality:** Limiting the functionality of systems to only the essentials needed for core operations is another step that helps throttle the actions of the SamSam group and others like it. If SMB isn't needed, disable it. The same can be said for RDP and other network services. ◆

*–Steve Ragan*

> If the SamSam crew is successful in its efforts to encrypt your systems, **your problems started long before any ransomware infection.**

# Two incident response phases most organizations get wrong

*It's important to remember:* ***Incident response isn't a thing, it's a process.***

**THERE IS A BASELINE** for incident response — six phases familiar to anyone who has spent time around a SANS classroom.

Those phases — preparation, identification, containment, eradication, recovery, and lessons learned — define the basic outline constructed to help a business manage a situation while keeping damage and recovery time to a minimum.

But there are some aspects to this baseline that organizations routinely get wrong.

Coming up in IT, this reporter was introduced to SANS by a mentor, and while this is not a sponsored post, I don't shy away from the fact that I'm a fan of the organization, as well as several of its instructors.

Today's article will focus on a conversation Salted Hash had with Rob Lee, the DFIR curriculum lead at SANS last month. (You might remember him from episode 15 of Salted Hash posted earlier this year.)

While interviewing those impacted by a string of recent ransomware attacks, I was reminded that incident response is a living process that changes constantly depending on the situation.

Most organizations either offer or rely on SaaS platforms to function, and many of the incident response plans they have in place don't really adapt to fluid environments such as those.

Instead they're focused on the static environments of the early 2000s (or older). While there is a good deal of crossover, there are little things that can trip an organization up, harming their reputation as well as their bottom line if they're not careful.

With that said, I started the conversation by asking about what's not getting enough attention when it comes to the baseline? Where are the gaps?

"The biggest gap that I see initially is a failure to understand that incident response is a process, it's not a thing," says Lee. "You don't do incident response, you do a phase of incident response."

In addition, there is a failure to understand the difference between containment and eradication. "Many people feel that if you go directly to eradication, we're essentially achieving containment because we're eradicating at the same time," Lee adds.

But they're not.

## Containment

The reason containment exists, Lee says, is that it gives incident response teams time to do proper scoping of the incident. This goes back to the identification phase, which some organizations confuse. The identification phase isn't about intrusion detection, it's about determining how bad the cancer is within your organization.

You have to find every location with infection. If you don't, the adversary or infection will maintain its foothold on the network, even if all six

> Many people feel that if you go directly to eradication, **we're essentially achieving containment** because we're eradicating at the same time.
>
> **ROB LEE,** DFIR CURRICULUM LEAD, SANS

phases are followed and completed.

To put it another way, containment is essentially heavy monitoring with the ability to get in the way of the final goals or objectives of the adversary, which really makes organizations feel nervous, Lee explained.

"During this stage you're still mapping out and learning about the adversary. You're learning about how bad the infection is. But it feels like you're doing nothing, you're just watching. And that's one of the hard parts in most organizations," Lee said.

"Unless you've been in law enforcement, you have a really hard time making that connection that says containment is there for a reason, it gives you the ability to make sure you've fully scoped out everything and the ability interdict if something really bad is about to happen. But if you don't do that step properly and move immediately to eradication... you've essentially accomplished nothing. You're back at square one again."

**It takes incredible self-awareness for an organization to admit they failed** and own up to the fact they have to do better in the long run.

## Recovery

The second gap in most incident response programs centers on recovery and lessons learned. Most organizations, Lee said, are really failing here.

"They almost always feel that how they were attacked, or how the situation occurred in the first place was anomalistic," Lee explained.

But it wasn't just bad luck that led to the incident in the first place. These organizations aren't taking the opportunity to say 'listen, the likelihood of this occurring again is extremely high' — a true statement in today's environment.

"They don't take the time to say 'what, truly, did we do to make sure that we have not only recovered from the previous incident, but we have enough in play to detect and defeat the second one?'," Lee added.

Once an organization is known to be vulnerable, the odds are stacked against it as other bad actors line up to take their shot. Not to mention, dealing with the same bad actors again.

"The likelihood that an adversary, if they were not able to meet their initial objectives, will potentially come back a second time is almost near one-hundred percent," Lee said.

It takes incredible self-awareness for an organization to admit they failed and own up to the fact they have to do better in the long run, which is why the recovery and lessons learned phases are so important. Achieving this level of awareness, though, will require some cultural changes within the organization.

After an incident, most organizations focus on patching or adding additional layers of intrusion detection, forgetting about the root cause of the problem.

You actually have to go back and measure some things during those initial stages. For example, how long has that breach been there before you detected it? Doing so is a metric known as dwell time to many in the industry.

"If you're not reducing your dwell time every single time another incident occurs, then that shows there's a more systemic problem in your organization in dealing with intrusion detection in the first place," Lee said.

Interestingly enough, most organizations don't talk about dwell time. Rarely will you see an organization discuss how many incidents they deal with in a given year and how quickly they can respond.

## Lessons learned

Bottom line? Incident response is a loop, and for the most part you're always in the lessons learned phase. "So, you'll never actually finalize the loop," Lee said. "You're actually moving back into the identification phase thinking, 'something else is going to happen, can we find it?'"

This is where incident response becomes a security model that most organizations don't just pick up and dust off when a bad thing happens, Lee added. It becomes what they use on a daily basis.

In fact, he said, those in the security industry who have adopted incident response as a day-by-day task, end up faring better than those who resort to a dusted off incident response manual that was created two to three years ago. ◆

*Steve Ragan is Senior Staff Writer at CSO.*