The True Cost of Ransomware

5 Companies, 5 Attacks, and the Reality of Recovery

Barkly®

Table of contents

Intro

When it comes to the ransomware attacks we see in the news, we seldom get the full story. Attacks don't start with ransom notes suddenly appearing out of nowhere, and their true impact doesn't stop with victims buying decryption keys or recovering files from backup.

As a result, the reality of ransomware is often far different than what we imagine and plan for. Infections can happen in the blink of an eye, yet the fallout from them can stretch out in unexpected ways — for days, weeks, sometimes months.

In the following five stories you'll get a special behind-the-scenes look at how ransomware infections played out inside five very different organizations. You'll understand the true cost of the attacks on their businesses, and receive key takeaways that can help you prepare your own organization for what a possible infection would really entail.

How one ransomware attack cost a Buffalo, NY hospital $10,000,000

How the attack unfolded

It started in the early hours of Sunday, April 9th. It was 2am, a time when most organizations' offices sit silent and dark. That was far from the case at Erie County Medical Center, a 602-bed hospital in Buffalo, NY, however. As the region's Level 1 trauma center, the emergency room in particular would have been a whirlwind, packed with patients and staff treating anything from car crashes to major burns to gunshot wounds and the other types of extreme injuries that keep the department operating over-capacity an average of 12 hours a day.

In the midst of all that activity, it may have taken a few moments for staff to register the fact that strange message windows had silently popped up on computer screens all across the hospital. One second they weren't there, and it was just another hectic overnight weekend shift. The next, there they were — ransom notes announcing the hospital's files had been encrypted, and the only way to unlock them was to pay 24 Bitcoins, roughly $30,000.

An hour and a half later, the medical center's IT team made the decision to shut all computer systems down. From that point forward — for a period lasting more than six weeks — ECMC would be forced to meet all the modern-day demands of a major urban hospital by relying on low-tech, manual processes, some of which hadn't been used in 20 years.

VICTIM
Erie County Medical Center

RANSOMWARE
Samsam

DATE OF ATTACK
April 9, 2017

LENGTH OF RECOVERY
More than six weeks

COST OF RECOVERY
$10,000,000

ATTACK FALLOUT

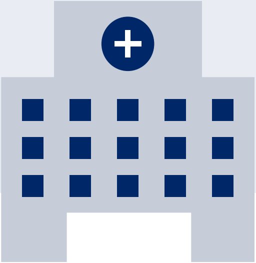
6,000 computers wiped, restored, and redistributed

Patient notes written and circulated by hand for 4 weeks

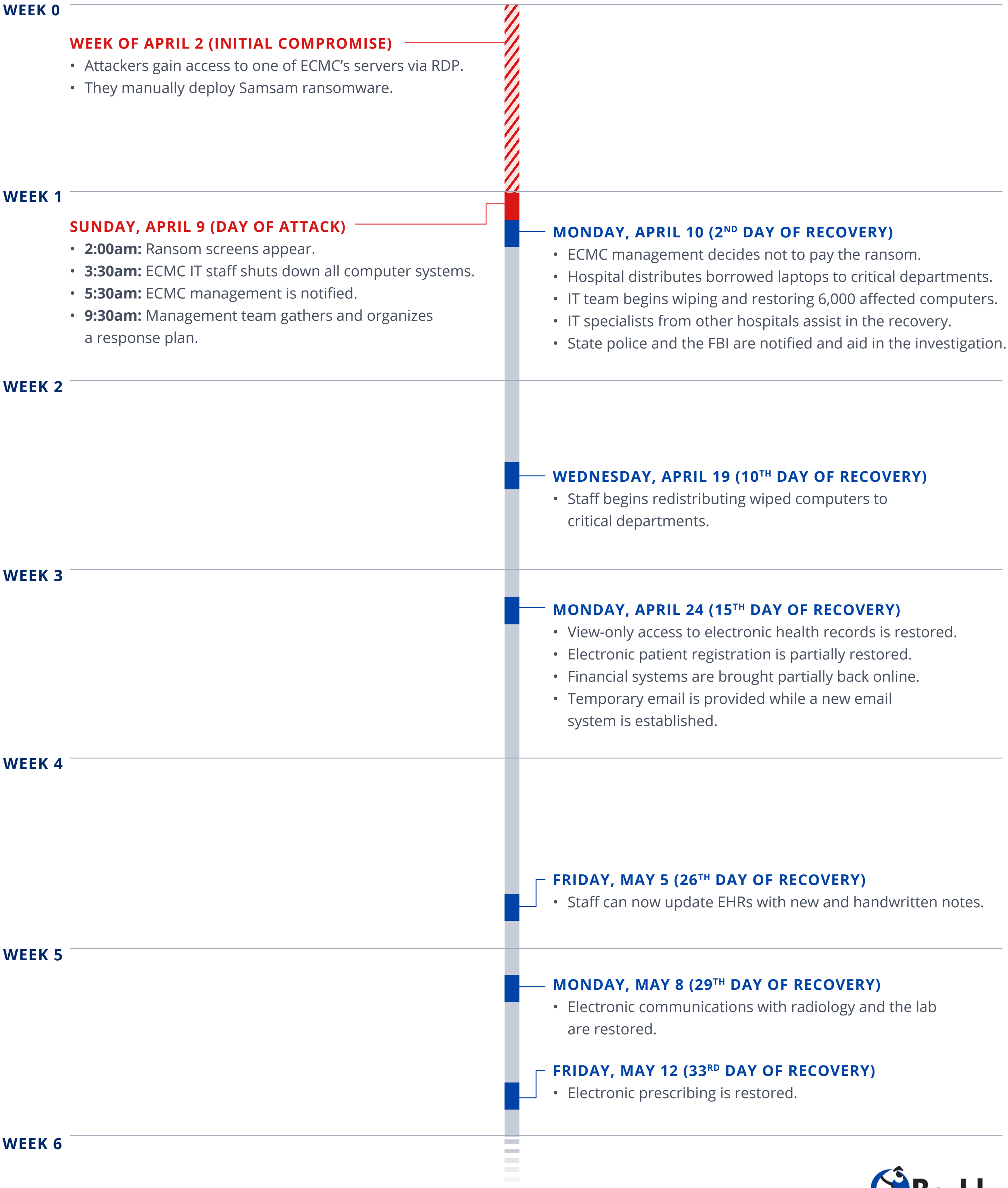
2 weeks of limited email and no electronic patient registration

3 weeks without electronic communication with the hospital lab

Full month without electronic prescribing



Infection and recovery timeline



WEEK 0

WEEK OF APRIL 2 (INITIAL COMPROMISE)

- Attackers gain access to one of ECMC's servers via RDP.
- They manually deploy Samsam ransomware.

WEEK 1

SUNDAY, APRIL 9 (DAY OF ATTACK)

- **2:00am:** Ransom screens appear.
- **3:30am:** ECMC IT staff shuts down all computer systems.
- **5:30am:** ECMC management is notified.
- **9:30am:** Management team gathers and organizes a response plan.

MONDAY, APRIL 10 (2ND DAY OF RECOVERY)

- ECMC management decides not to pay the ransom.
- Hospital distributes borrowed laptops to critical departments.
- IT team begins wiping and restoring 6,000 affected computers.
- IT specialists from other hospitals assist in the recovery.
- State police and the FBI are notified and aid in the investigation.

WEEK 2

WEDNESDAY, APRIL 19 (10TH DAY OF RECOVERY)

- Staff begins redistributing wiped computers to critical departments.

WEEK 3

MONDAY, APRIL 24 (15TH DAY OF RECOVERY)

- View-only access to electronic health records is restored.
- Electronic patient registration is partially restored.
- Financial systems are brought partially back online.
- Temporary email is provided while a new email system is established.

WEEK 4

FRIDAY, MAY 5 (26TH DAY OF RECOVERY)

- Staff can now update EHRs with new and handwritten notes.

WEEK 5

MONDAY, MAY 8 (29TH DAY OF RECOVERY)

- Electronic communications with radiology and the lab are restored.

FRIDAY, MAY 12 (33RD DAY OF RECOVERY)

- Electronic prescribing is restored.

WEEK 6

Attack fallout

Taking into account advice from law enforcement authorities and security experts, ECMC management decided not to pay the ransom. The only way to maintain the integrity of its systems and ensure the attackers hadn't made any additional malicious changes was to wipe all the potentially affected machines and restore each from from backups conducted before the initial compromise occurred.

As ECMC's IT staff worked with external specialists around-the-clock to carry out that task and get the hospital's computer system back up and running, the rest of the staff grappled with the challenges of conducting their work offline. Practically everything that needed to be done took more time. And for a hospital specializing in urgent care and trauma, more time is the one thing no one ever has.

In July, three months after the attack, ECMC estimated the total costs associated with the incident had reached nearly $10 million. Roughly $5 million had been spent on "computer hardware, software, and assistance needed in the response," while loss of revenue and increased expenses such as overtime pay added up to an additional $5 million in damages.

Key takeaways

1) Securing Remote Desktop Protocol (RDP) should be a top priority
Ransomware attacks are often attributed to users opening malicious email attachments or visiting compromised websites, but the truth is the biggest uptick in successful ransomware attacks against hospitals involves attackers breaking into networks via RDP.

All attackers have to do is scan the Internet for systems with port 3389 exposed and then launch a brute-force attack to crack weak or default passwords to gain access and execution. That makes scanning hospital networks to determine whether any machines have port 3389 open a top priority. Tools like Nmap can make that process easy. Organizations should just keep in mind attackers have access to these types of tools, as well.

2) An ounce of prevention is worth a pound of cure

Attacks like this one and WannaCry's infection of the UK's National Health Service (NHS) in May are potent examples of just how damaging and disruptive ransomware can be once it's set loose inside a hospital network.

It's clear that, when it comes to ransomware, detecting and responding to attacks after the fact is no longer enough. Organizations need to prioritize preventing infections at the outset, before they have a chance to do damage. In addition to securing vulnerable ports, that also means supplementing standard antivirus solutions with newer forms of protection on the endpoint. Learn how Barkly goes beyond antivirus to keep companies protected against the latest ransomware attacks.

3) Have a response plan ready

When ransomware infections happen, there isn't much time to react. And in a setting like a hospital emergency room, there's certainly no option to hit pause while you assess the situation and come up with a plan. Disaster preparedness played a key role in ensuring the disruption at ECMC wasn't even worse. The key for other providers is to make sure they have a practiced plan in place before they need it, too.

How one of the world's largest law firms was paralyzed by Petya

How the attack unfolded

On the morning of Tuesday, June 27th, employees arriving at the DC offices of DLA Piper, one of the world's largest law firms, were greeted with something unusual. A whiteboard had been rolled out into the middle of the building lobby with "Attention: DLA Employees" written across it in large, red letters.

"All network services are down, DO NOT turn on your computers!" the message continued. "Please remove all laptops from docking stations & keep turned off. No exceptions."

As the DC office employees slowly filed past the whiteboard wondering what was going on, text message notifications were urgently being sent out alerting the rest of the firm's employees not to start their computers or connect to the DLA network, either.

The phone systems were down. So was email and the firm's web portal. Without access to communications or documents, operations ground to a halt.

Initial details were scarce, but what eventually became clear was, like thousands of other organizations around the globe, the firm had been infected by Petya malware. As a result, the entire firm — roughly 3,600 lawyers plus support staff scattered across 40 countries — was on digital lockdown.

What no one at DLA Piper knew or anticipated on that chaotic first day of the outbreak was that the lockdown wouldn't be fully remediated for weeks to come.

VICTIM
DLA Piper

RANSOMWARE
NotPetya (technically a wiper)

DATE OF ATTACK
June 27, 2017

LENGTH OF RECOVERY
At least two weeks

COST OF RECOVERY
Millions

ATTACK FALLOUT
Full day without phones

6 days without email

2 weeks without access to key documents

Infection and recovery timeline

WEEK 1

TUESDAY, JUNE 27 (DAY OF THE ATTACK)

- **5:48am:** Reports of a major cyber attack first reported targeting companies primarily in Ukraine.
- **6am:** DLA Piper's Madrid office experiences signs of infection and is immediately locked down.
- **7:37am:** DLA Piper's phone lines are reported down.
- **7:55am:** The firm's web portal, used to access sensitive documents, is reported down.
- **Tuesday morning:** Firm employees instructed via text message alert system not to start their computers or connect to the DLA network.
- **9:36am:** Firm confirms malicious activity on its network appears to be related to Petya outbreak, says IT team acted quickly to prevent the spread.
- **10am:** Photo of whiteboard outside the firm's D.C. office is posted on Twitter.
- **Tuesday afternoon:** Firm employees are instructed via text to leave at 3pm.

WEDNESDAY, JUNE 28 (2ND DAY OF RECOVERY)

- **6:42am:** Firm announces it is working with external forensic experts and relevant authorities.
- **Wednesday morning:** Firm alerts employees offices are open, phones are working, and email should be back up within hours.
- **Wednesday evening:** New assessment is email will be up by Thursday morning.

WEEK 2

MONDAY, JULY 3 (7TH DAY OF RECOVERY)

- **1am:** Firm announces email is up, but other systems are still being restored.
- Firm says there is no evidence client data was exfiltrated or compromised.

THURSDAY, JULY 6 (10TH DAY OF RECOVERY)

- **Thursday morning:** Emails sent or received prior to the attack still inaccessible.
- Some staff still unable to access key documents directly.

THURSDAY, JULY 6 (10TH DAY OF RECOVERY)

- **Thursday afternoon:** Firm offices are open and it is advising clients.

WEEK 3

MONDAY, JULY 10 (14TH DAY OF RECOVERY)

- **4:35am:** Firm thanks clients and partners for their patience while recovery efforts continue.

Attack fallout

It can be difficult to fully appreciate just how debilitating and disruptive an incident like the NotPetya outbreak truly was for any organization, let alone a major global law firm with a huge roster of multinational clients.

> *"Consider litigators unable to access motions on a deadline. Trial lawyers preparing for arguments without key documents. Transactional lawyers unable to communicate with clients attempting to close multibillion-dollar deals."*
>
> **— Roy Strom, The Am Law Daily**

According to insurance brokers, the total direct and indirect costs associated with the attack on DLP Piper could be in the millions.

Key takeaways

1) With ransomware, detection often comes too late

According to the firm, its IT team was able to act quickly to prevent the spread of NotPetya thanks to an alert from its "advanced warning system" that suspicious activity had been detected on the network. Unfortunately, being alerted that you're locked out after the fact isn't an ideal scenario. When it comes to ransomware, blocking attacks at the very outset with protection that works at runtime is crucial.

2) Everyone has a plan until you get punched in the face

Even for extremely practiced organizations — DLA Piper reports it has assisted numerous companies in responding to and recovering from cyber attacks — mitigation can take time and be one heck of a bumpy ride. Not only do you need a plan, you need to be prepared to adjust and react when things don't according to that plan.

3) No firm or organization is immune

The third takeaway comes from from Larry Ponemon, chairman and founder of the Ponemon Institute, a research think tank specializing in data protection. Ponemon has worked with DLA Piper as a consultant and considers its data privacy and security measures to be very strong.

"From my experience, [DLA Piper] is an excellent firm with reasonable due diligence procedures," Ponemon says. "This tells me...this could happen to anyone."

How ransomware took San Francisco's PBS station offline

How the attack unfolded

The day at KQED began like most others, with reporters busy connecting with sources, compiling stories and preparing to broadcast. But, late that afternoon, IT detected unusual activity on the network. Hours later, the email server stopped working. Clearly, there was a major problem.

IT immediately instructed all employees to shut down all connected devices to thwart propagation, and they did it the old-fashioned way: with handwritten signs posted around the office. Some staff were sent home and the rest were told not to use or turn on their computers. The livestream broadcast dropped Thursday night, and wasn't back on until 9:30 a.m. the next morning.

With files locked down, either by the ransomware or as defensive measure, work came to a virtual standstill. The hackers demanded 1.7 Bitcoin per infected computer (at the time roughly $3,600). Instead of paying, the station called the FBI.

VICTIM
Public TV and radio station KQED

RANSOMWARE
Mole

DATE OF ATTACK
June 15, 2017

LENGTH OF RECOVERY
Over a month

COST OF RECOVERY
Undetermined

ATTACK FALLOUT

12 hours of dead air on the station's online broadcast

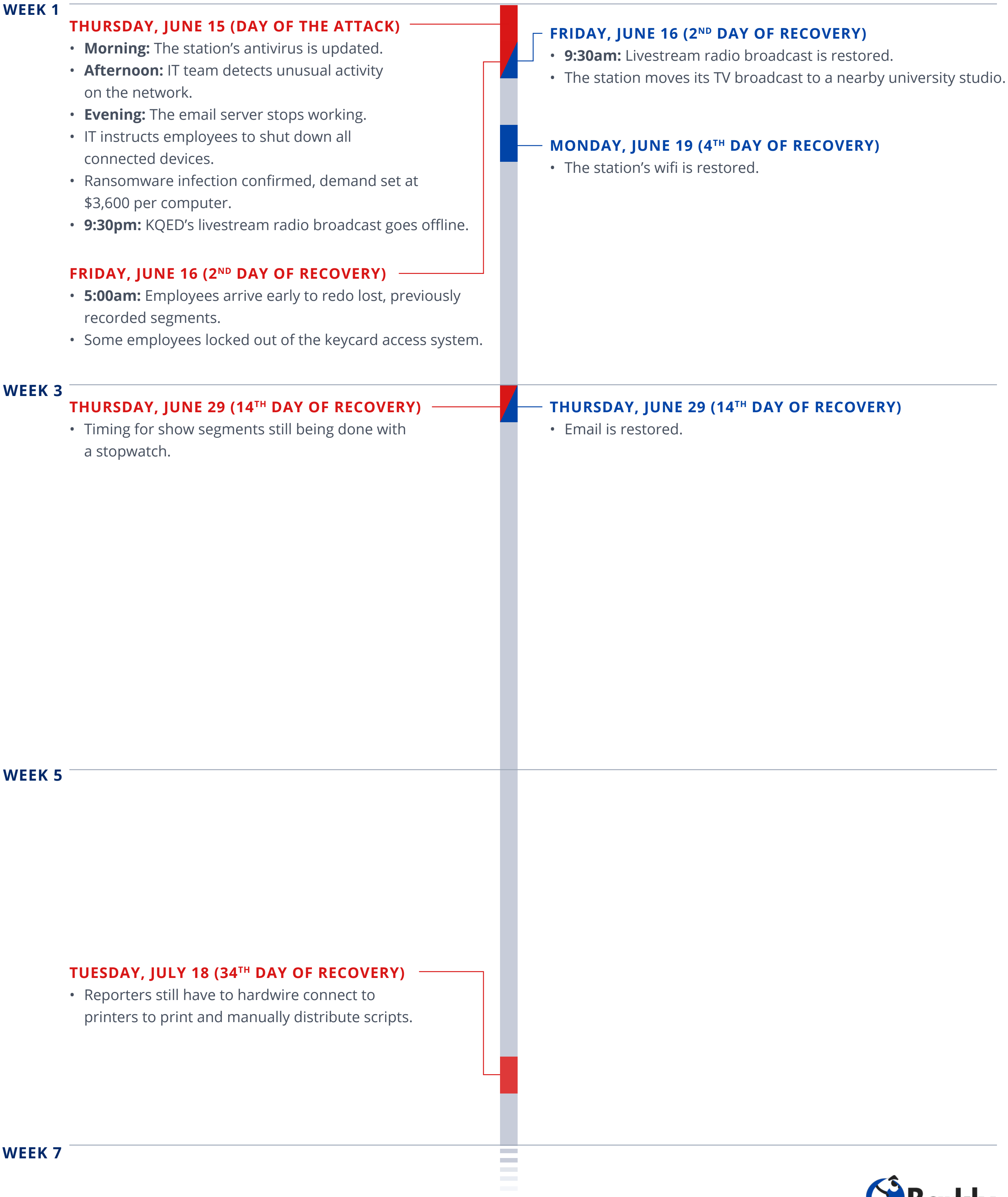
Loss of pre-recorded segments

2 weeks without email

TV broadcast moved to nearby university studio

Loss of access to the station's content management platform and access card system

Infection and recovery timeline



WEEK 1

THURSDAY, JUNE 15 (DAY OF THE ATTACK)

- **Morning:** The station's antivirus is updated.
- **Afternoon:** IT team detects unusual activity on the network.
- **Evening:** The email server stops working.
- IT instructs employees to shut down all connected devices.
- Ransomware infection confirmed, demand set at $3,600 per computer.
- **9:30pm:** KQED's livestream radio broadcast goes offline.

FRIDAY, JUNE 16 (2ND DAY OF RECOVERY)

- **9:30am:** Livestream radio broadcast is restored.
- The station moves its TV broadcast to a nearby university studio.

MONDAY, JUNE 19 (4TH DAY OF RECOVERY)

- The station's wifi is restored.

FRIDAY, JUNE 16 (2ND DAY OF RECOVERY)

- **5:00am:** Employees arrive early to redo lost, previously recorded segments.
- Some employees locked out of the keycard access system.

WEEK 3

THURSDAY, JUNE 29 (14TH DAY OF RECOVERY)

- Timing for show segments still being done with a stopwatch.

THURSDAY, JUNE 29 (14TH DAY OF RECOVERY)

- Email is restored.

WEEK 5

TUESDAY, JULY 18 (34TH DAY OF RECOVERY)

- Reporters still have to hardwire connect to printers to print and manually distribute scripts.

WEEK 7

Attack fallout

> *"It's like we've been bombed back to 20 years ago, technology-wise."*
> **— Queena Kim, KQED Senior Editor**

Following the infection and initial live streaming dead air, the staff at KQED went to extraordinary lengths to ensure broadcasts aired uninterrupted. Employees came in early to re-record lost segments, they developed workarounds, using stopwatches to time segments and hardwire connecting to printers so they could print and distribute scripts by hand.

"We've basically been putting everything together with duct tape for a month," said KQED reporter Marisa Lagos. "From an outside point of view, we really made it work. But what our listeners don't know is that people have been doing really crazy things to make sure no one notices that anything is wrong."

Meanwhile, IT staff was scrambling to wipe all infected machines and reinstall operating systems — a slow, cumbersome process that has consumed a tremendous amount of resources and time.

Key takeaways

1) Ransomware infections can have huge ripple effects
When we think of ransomware we tend to focus on the fact that it encrypts files. But the truth is, when an infection hits an organization, files aren't just encrypted. Systems that depend on access to those files break.

"You rely on technology for so many things," KQED's Kim acknowledged, "so when it doesn't work, everything takes three to five times longer just to do the same job."

2) The most damaging effect is often loss of productivity
Ransom demand amounts tend to figure prominently in coverage of attacks, but the truth is they are often dwarfed by the costs of recovery, downtime, lost business, and dramatic drops in productivity. Even with staff working around the clock to mitigate the situation and come up with creative workarounds, the hours spent unable to conduct business as usual can cause profits to plummet.

3) Traditional security isn't enough

Adding salt to the wound, KQED had reason to believe they should have been protected from an infection like this — at least by traditional measures. The station's CTO reported AV systems had just been updated that very morning, and its firewalls, email scanning, and multiple malware detection programs were all in place and up-to-date, as well. But because the ransomware was a new variant, it slipped past them all.

And, therein lies the real problem: when it comes to protecting an organization against ransomware or other malware, standard signature-based security software can only detect known variants, leaving a major gap that needs to be addressed. The potential costs of not doing so are too prohibitive.

How ransomware cost an Idaho county $100,000

How the attack unfolded

On February 15, employees for Bingham County, Idaho, discovered they were locked out of crucial systems involved in dispatching emergency responders. IT staff were called in at 4am to assess the situation, and they quickly learned ransomware had encrypted the county servers.

After investigating, they determined attackers had been able to find an open port 3389 on the county's servers that was exposing Remote Desktop Protocol (RDP) to the internet. From there, it was simply a matter of using a brute force attack to crack the password, then the criminals had access to deploy their ransomware on the servers manually.

With data on the servers encrypted, computer systems across every department in the county were affected.

VICTIM
Bingham County, Idaho government

RANSOMWARE
Samsam

DATE OF ATTACK
February 15, 2017

LENGTH OF RECOVERY
Estimated to be a year or longer

COST OF RECOVERY
$100,000

ATTACK FALLOUT
Complete rebuild of servers

Every department in the county affected

$3,500 in paid ransom

Emergency dispatchers had to use physical maps to direct officers

Thousands of radio transmissions, calls, and police reports logged manually

Infection and recovery timeline

WEEK 1

WEDNESDAY, FEBRUARY 15 (DAY OF THE ATTACK)

- County emergency dispatchers discover they can't access crucial systems.
- **4:00am:** IT staff called in to investigate.
- Computer and phone systems down across the county.
- Ransomware infection discovered.
- Decision made not to pay $28,000 ransom.
- IT team begins wiping and restoring infected servers from backup.

FRIDAY, FEBRUARY 17 (3RD DAY OF RECOVERY)

- IT discovers data on 3 infected servers could not be recovered.
- County pays attackers $3,500 for decryption keys for those 3 servers.

FRIDAY, FEBRUARY 17 (3RD DAY OF RECOVERY)

- 25 of the county's servers have been restored via backup.

TUESDAY, FEBRUARY 21 (7TH DAY OF RECOVERY)

- While computer systems are being restored county employees keep written records by hand.

WEEK 3

WEDNESDAY, MARCH 1 (15TH DAY OF RECOVERY)

- Recovery costs reach nearly $100,000.
- IT team estimates it could take until 2018 to be 100% recovered.

WEDNESDAY, MARCH 1 (15TH DAY OF RECOVERY)

- County reports its systems are 90% back to normal.

Attack fallout

County officials initially sought to avoid paying the ransom, believing they would be able to recover all the encrypted data thanks to having multiple backup systems in place. Unfortunately, three servers could not be restored from backup.

In order to recover the information on those three servers, the county paid three Bitcoin, at that time roughly $3,500, and were provided the decryption key. Even with the key, however, restoring the servers from backup and getting everything back to normal became an ongoing task consuming considerable time and resources.

While IT staff pulled all-nighters and worked weekends, the rest of the county employees were forced to conduct paperwork by hand, writing out court proceedings, dispatch calls, and other records that would have to be transcribed back into the computer systems as they came back online.

Two weeks into the recovery process, costs had already reached $100,000 and the IT team estimated it could take up to nine months to get the systems 100 percent back to normal.

Key takeaways

1) Backups aren't foolproof
Backup is best thought of as a last resort. You should hope you never have to rely on it, but you also should be confident enough in your implementation that if you do need it, it will come through.

The best way to do that is by practicing 3-2-1 backup. That means keeping three copies of your data stored on two different types of media, one of which is offsite. Organizations should also adhere to the principle of "Schrodinger's backup" — the condition of any backup is unknown until a restore is attempted. In other words, the only way you can actually know whether restoring data from backup will work is by doing it.

Bottom line: Make sure your backup coverage actually accounts for all of your servers and devices, and make sure you actively test your backups regularly.

2) Paying the ransom doesn't immediately make the problem go away
Despite being able to restore the majority of the encrypted data from backup and purchase decryption keys for the rest, the Bingham County IT team still had to completely rebuild their servers, not to mention make adjustments to prevent repeat attacks.

A considerable portion of the county's recovery costs were made up of overtime pay for both the IT team as well as additional employees tasked with transcribing the hand-written records taken while computer systems were offline. Paying the ransom didn't make any of that work less necessary or those costs go away.

3) Account lockout policies can help protect against brute-force attacks
The attack on Bingham County is another example of criminals taking advantage of failure to properly secure Remote Desktop Protocol (RDP). Once criminals discovered a server with RDP exposed they were able to gain access by brute-forcing the login. You can make that process more difficult for attackers by implementing an account lockout policy, where, after a certain number of failed login attempts, accounts get locked down.

Behind the largest ransomware payout in history

How the attack unfolded

On June 10, employees at South Korean web hosting company Nayana made a nightmare discovery. Their servers had been infected with ransomware, and now all their data — data more than 3,400 customers relied on to keep their websites up and running — was encrypted. In a series of agonizing updates, the company chronicled how it discovered its backups of the data were encrypted, as well, leaving them with no option but to negotiate with the attackers.

The starting demand, however, was a staggering $4.4 million. Over the next few days, Nayana's CEO went back and forth with the attackers, eventually talking them down to $1 million, which the company agreed to pay in three installments.

Over the course of the next month, the company's challenge would be investigating, restoring, and backing up decrypted data on 153 servers, all while asking its customers for continued patience during the downtime. The initial assessment was that, upon receiving the decryption keys, each server would be back up and running in two weeks. But as Nayana would find out, that assessment was incredibly optimistic.

VICTIM
Web hosting provider Nayana

RANSOMWARE
Erebus

DATE OF ATTACK
June 10, 2017

LENGTH OF RECOVERY
Over a month

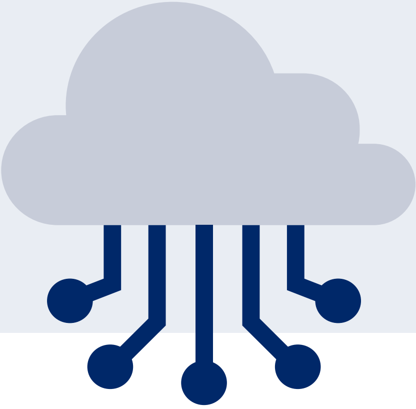
COST OF RECOVERY
$1,000,000 in paid ransom, total cost undetermined

ATTACK FALLOUT
Data on 153 servers encrypted

Websites belonging to 3,400 customers affected

Affected customers issued 3 months free service and 30% discount in perpetuity

Customers with unrecoverable loss data given free service in perpetuity



Infection and recovery timeline

WEEK 1

SATURDAY, JUNE 10 (DAY OF THE ATTACK)

- Nayana discovers its servers infected with ransomware.
- Company reports the attack to the Korea National Internet Development Agency (KISA).
- 153 servers are infected with Erebus ransomware.
- Backups of the data confirmed encrypted, as well.
- Nayana begins negotiations with attacker to purchase decryption keys.

SUNDAY, JUNE 11 (2ND DAY OF RECOVERY)

- Attacker makes "final" demand of 5.4 Bitcoin per server with deadline of June 14th.

WEDNESDAY, JUNE 14 (5TH DAY OF RECOVERY)

- Nayana CEO reports demand was negotiated from $4.4 million to $1 million.

THURSDAY, JUNE 15 (6TH DAY OF RECOVERY)

- Nayana announces ransom will be paid in three installments, with attacker sending decryption keys after each payment.
- Company estimates two weeks recovery time once each server is decrypted.

WEEK 2

SATURDAY, JUNE 17 (8TH DAY OF RECOVERY)

- Errors in attacker's decryption program slow recovery process.

SATURDAY, JUNE 17 (8TH DAY OF RECOVERY)

- 49 servers decrypted, six of which back up and running after integrity check.

TUESDAY, JUNE 20 (11TH DAY OF RECOVERY)

- Company issues revised estimate that recovery will extend into July.

THURSDAY, JUNE 22 (13TH DAY OF RECOVERY)

- Nayana CEO confirms third payment made and all decryption keys delivered.

WEEK 3

THURSDAY, JUNE 29 (20TH DAY OF RECOVERY)

- Several servers determined unrecoverable.
- Company also reports Korean language documents cannot be decrypted.

THURSDAY, JUNE 29 (20TH DAY OF RECOVERY)

- 125 of the 153 infected servers decrypted.

WEEK 4

THURSDAY, JULY 6TH (27TH DAY OF RECOVERY)

- Nayana confirms all servers decrypted, but some files corrupted or unrecoverable.

THURSDAY, JULY 6TH (27TH DAY OF RECOVERY)

- Affected customers offered three free months of web hosting with permanent 30% discount thereafter.
- Customers with non-recoverable data loss offered free web hosting in perpetuity.

WEEK 5

Attack fallout

The attack on Nayana encrypted data on 153 servers, locking more than 3,400 customers out of data they needed to keep their websites up and running. In addition to paying $1 million in ransom to the attackers, the company suffered indeterminate business losses and potentially irreparable damage to its relationships with its customers.

After nearly a month of around-the-clock work, the company had to inform its customers that, due to a flaw in the attackers' decryption program, some data would be unrecoverable. Customers affected by the attack were offered three free months of web hosting, with a permanent 30% discount kicking in thereafter. Customers with non-recoverable data loss were offered free service in perpetuity.

Considering the staggering downtime, the cost of recovery, the loss of business, and the potential for customer law suits, Nayana's CEO acknowledged the future of the company is very much in jeopardy.

Key takeaways

1) Attackers are beginning to adjust ransom demands per victim
Ransomware has traditionally taken an indiscriminate "spray and pray" approach. Criminals have tried to distribute their attacks wide enough and priced their demands low enough to increase their odds of more victims paying. As the attack on Nayana shows, however, more and more ransomware criminals are directing their attacks to where the money is (big businesses), and adjusting their demands based on what they believe the victim will be willing and able to pay.

The fact that these criminals felt bold enough to make a multi-million-dollar demand suggests they knew the value of the data they had encrypted. And the fact that they successfully got $1 million will only encourage more attacks moving forward.

2) Criminals can't always be counted on to make software that works

Paying the ransom is an option no business wants to consider, but to make matters worse, there are plenty of cases where that option doesn't actually result in files getting decrypted. Criminals can't be trusted for a variety of reasons. As was the case with the criminals Nayana dealt with, their software can have flaws. Once you pay they may simply ask for more money. Or, they may never have the intention or ability to decrypt your files in the first place.

3) Patching is key

The malware responsible for infecting the Nayana servers was identified as a variant of Erebus ransomware. While the specific attack vector used to infect Nayana's servers was never officially confirmed, researchers suspect vulnerabilities in outdated systems and software was to blame.

Making sure all the machines in your organization are fully patched and up-to-date is easier said than done. The reality is deploying patches across enterprise environments can pose significant logistical challenges. There may be machines that you simply can't apply updates to for a variety of reasons. The next best solution is to segment these machines and reduce your risk by limiting what they have access to.

Don’t wait till you have to put out ransomware fires.

Stop them from starting in the first place.

Considering the downtime and recovery costs associated with ransomware infections (even when data is recoverable), prevention should be a priority for all organizations.

Find out how Barkly fills the gaps traditional endpoint security solutions like antivirus leave open by blocking even new, never-seen-before ransomware before it can do any damage.

Request a demo

About Barkly
Barkly’s Endpoint Protection Platform™ uses Responsive Machine Learning™ to uniquely block exploit-driven, fileless, and file-based attacks. Barkly delivers fast, lightweight protection, administered through an easy-to-use cloud service.

Learn more at barkly.com.

Barkly®