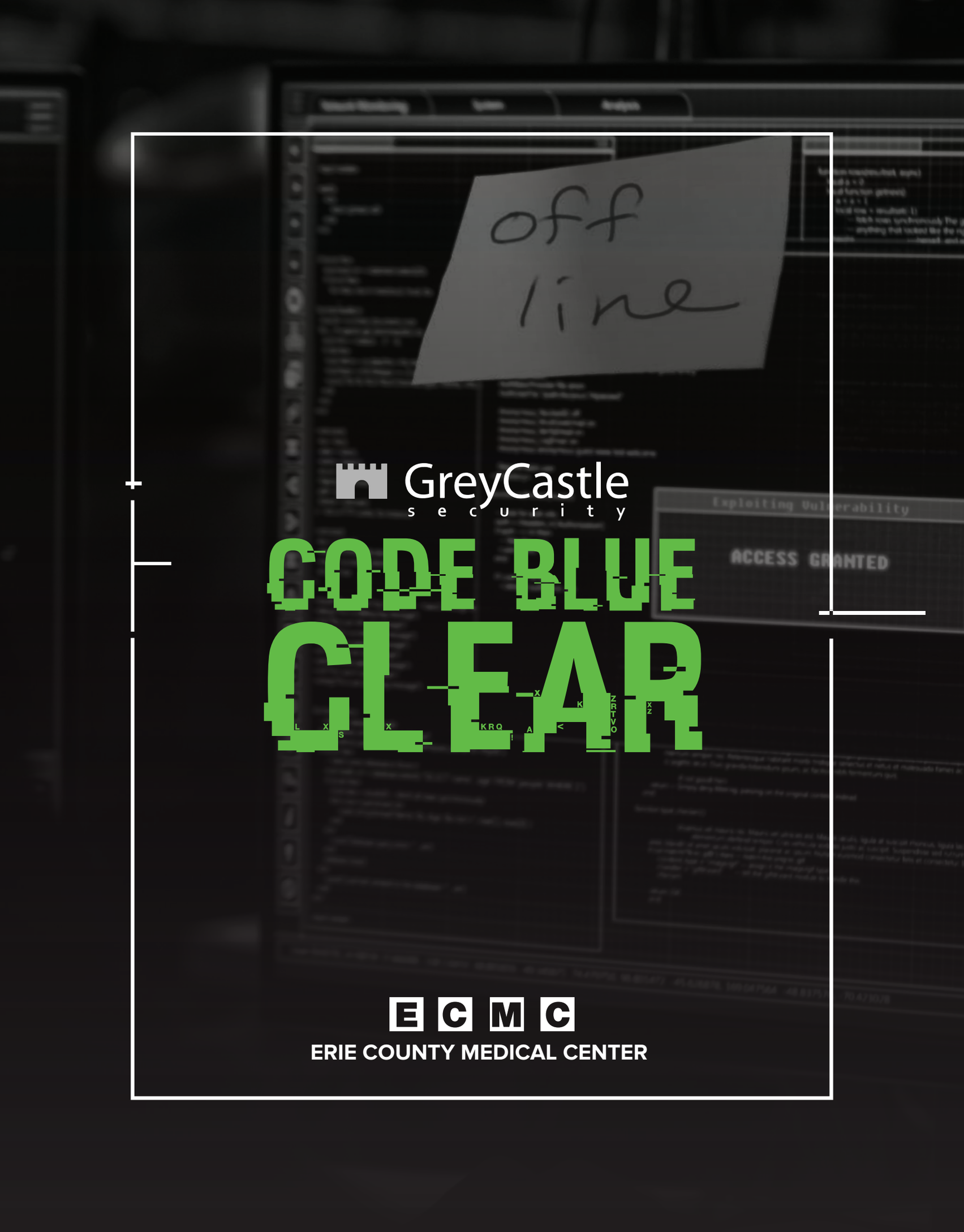


GreyCastle
security

CODE BLUE CLEAR

ECMC
ERIE COUNTY MEDICAL CENTER

Your PC ran into a problem that it couldn’t handle.

Your PC will restart in: 5 seconds

13 | days offline

400 | servers compromised

992 | hospital beds at risk

6000 | computers down

Add them up and you get the **largest ransomware attack in U.S. history,** endangering hundreds of lives and crippling an award-winning hospital in Upstate New York. The ransom payout was exactly zero dollars - but is this a zero-sum game?

It depends.

While the impact from this vicious ransomware attack was unprecedented, most experts agree that Erie County Medical Center's response was monumental – helping the organization avoid months of downtime and millions of dollars in losses.

AN EASY TARGET

Hackers have discovered that healthcare is an easy, lucrative target.

Healthcare organizations are the perfect target – identities, credit card transactions and health records, all in one convenient location. Additionally, healthcare organizations are faced with legacy software vulnerabilities, unpredictable budgets and a product that may mean life or death on any given day. Anonymous payment mechanisms, like Bitcoin, have made it even easier for hackers to cash in on these conditions.

“Exposure” is a word that hospitals and physicians don’t like to hear.

While healthcare organizations take great care to mitigate the risks associated with clinical threats, exposure to economic and technologic threats is only now becoming a priority. Unfortunately, an institution’s vulnerabilities often go undetected until their networks have sustained serious injury.

The infection occurred after blunt force trauma to the network.

Instead of employing typical phishing methods or sophisticated malware to gain access to ECMC’s network, hackers identified a simple vulnerability—and exploited it. They targeted an Internet-facing server, fingerprinted the asset and then “brute forced” the password. Once inside, the hackers were able to pivot and move laterally among other networked assets, planning their attack for over a one-week period.

The attack was comprised of several phases; reconnaissance, deployment and execution.

This required the installation of another form of malware:

Self-executing code that harvested user credentials by commandeering existing computer administration tools and using them to gain entry to other local and remote networks in ECMC’s system.

Approximately one week after the initial intrusion into ECMC’s system on April Fools’ Day 2017, the first ransom note appeared.

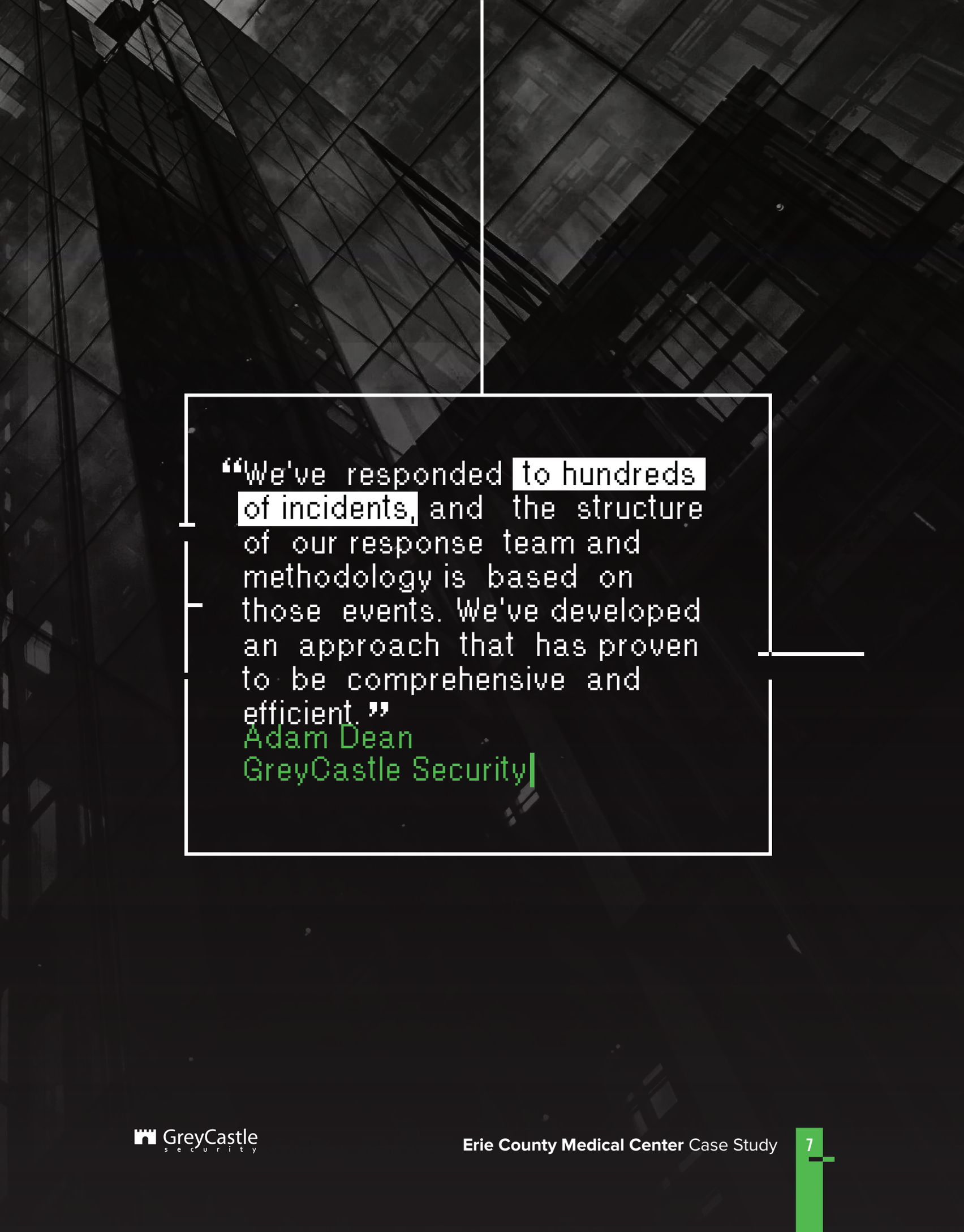
STEP 1

YOU MUST SEND US 1.7 BITCOIN FOR EACH AFFECTED PC OR 24 BITCOIN TO RECEIVE ALL PRIVATE KEYS FOR ALL AFFECTED PCS.

The hackers, connecting from various international locations in Brazil, Romania and the Netherlands, had encrypted ECMC's files and were demanding the current equivalent of $44,000 USD for the keys to unlock them. That's when ECMC shut down all of its computer systems and contacted GreyCastle Security, which promptly recommended ECMC not pay the ransom. Why?

"We knew that ECMC had tape backups of all their files, so even if the hackers had acquired or encrypted sensitive information, there was another copy. Plus, there's really no guarantee that the hackers would give us access to the files once they'd received the ransom," said Adam Dean, GreyCastle Security's Response Team Lead. In addition to its technical expertise, GreyCastle Security, based in Troy, New York, is known for its practical and risk-based approach to cybersecurity. "Cybersecurity is all we do," Dean pointed out. "Clients value our realistic and real-time approach to security, and knowing they can call us anytime, day or night, gives them peace of mind."

Mobilizing a Computer Incident Response Team (CIRT) for ECMC was the first task for GreyCastle Security. The team included a Response Team Lead, Incident Commander and Deputy Incident Commander, as well as experts specializing in digital forensics, investigations and networking.



> "We've responded to hundreds of incidents, and the structure of our response team and methodology is based on those events. We've developed an approach that has proven to be comprehensive and efficient."
>
> Adam Dean
> GreyCastle Security

CAPTURING TANGIBLE EVIDENCE

in a virtual world is like diagnosing a rare disease.

There are best practices and specialty tools that can be applied when responding to cyberattacks, but without highly developed problem-solving skills and insights, you'll still be stuck with only the symptoms.

"In regard to the level of sophistication, the attack on ECMC ranks in our top 10 percent," said Dean. "The manual intervention and the fact that someone was attempting exploratory surgery on the system made this incident unique. I think the combination of our methodology and our deductive capabilities is what allowed us to identify where the failures occurred and develop a remediation strategy so quickly."

TRIAGE

ECMC contacted GreyCastle Security at 5:30 a.m., Sunday morning, April 9, 2017—just two hours after discovering the attack. GreyCastle Security immediately began gathering information from both ECMC staff and through a cursory examination of ECMC's systems and networks.

ANALYSIS

Using the information gathered during triage, GreyCastle Security chose methods of analysis, including forensics, log inquiries, and network architecture and software audits, to determine the scope of the attack and extent of the damage. This, in turn, led to the identification of the ransomware and other malware the hackers installed. It was during this phase that GreyCastle Security ascertained no data or personal health information were exfiltrated or compromised during the attack.

CONTAINMENT

Knowing the malware variants, in addition to knowing how and where the intrusion occurred, GreyCastle Security took necessary action to neutralize the existing threat and prevent future damages.

ERADICATION

The attack affected more than 6,000 of ECMC's computers, all of which had to be scrubbed completely and have operating systems and applications reinstalled.

IDENTIFYING THE CAUSE

GreyCastle Security identified the root cause of the intrusion to be weak authentication credentials.

Just like a chain is only as strong as its weakest link, one overly simple password can negate the strength of even the strongest password on the network. Once the initial intrusion occurred, the attacker was able to obtain and use the credentials of higher-level administrators to spread and encrypt the ransomware system wide. While the ransomware was able to self-deploy, it did not have the capability to search, access, or exfiltrate confidential files, and did not make outbound connections.

The prognosis is good, but preventative measures must be taken to protect ECMC from another attack.

GreyCastle Security, following the successful remediation of the intrusion, presented ECMC with a list of recommendations—just as it does after every cybersecurity incident.

On their own, each of these recommendations will reinforce ECMC's systems and networks against potential intrusions. But when they're implemented in conjunction with one another, the durability of their systems will increase exponentially.

- Conduct a HIPAA risk assessment
- Perform regular internal and external vulnerability assessments
- Block all known malicious IP addresses
- Restrict permissions
- Restrict remote desktop connection
- Improve monitoring and logging
- Develop and enforce password policies

PREVENTING FUTURE INTRUSIONS

Cyberthreats targeting healthcare institutions will likely increase.

With incident response services provided by GreyCastle Security, ECMC was able to not only avoid paying ransom to the attackers, but also minimize the potential damage of the intrusion.

Furthermore, the identification of additional vulnerabilities of the hospital's systems and networks means that the likelihood of a similar attack is minimized. And that's not only good for outcomes, it's good for patients.

Cyberthreats targeting healthcare institutions will likely increase. With global ransomware attacks like WannaCry and NotPetya on the rise, it's imperative that all organizations —not just those in healthcare—take the necessary precautions to protect their computer systems, and their patients and customers. Ransomware attacks in the healthcare sector alone are expected to quadruple by 2020. The cost of a ransomware attack is not just limited to the ransom demands. The collateral damage associated with restoring files, software, and systems, and to preventing future intrusions, also proves costly.

FOR MORE INFORMATION ABOUT GREYCASTLE SECURITY AND ITS CAPABILITIES

GreyCastle security

www.greycastlesecurity.com
518.274.7233
intel@greycastlesecurity.com