The Ransomware-as-a-Service Evolution Is Here, with Its Sights on Your Mainframe
Companies healthcare providers never thought would operate in the healthcare environment are jumping in full-force and the disruption is all around us. For traditional healthcare organizations with a solid IT foundation, disruption is welcomed, benefiting from these new players in the market, while also safeguarding their position in the marketplace. BMC helps traditional healthcare organization embrace the disruption with the Autonomous Digital Enterprise that delivers agile Workflow Orchestration, Capacity Management and Mainframe Optimization, ensuring when disruption hit, healthcare organizations are ready.

The Ransomware Outbreak

In 1989, a biologist and consultant for the World Health Organization (WHO) named Joseph Popp assembled a mailing list of healthcare professionals and sent out thousands of 5.25-inch floppy disks. He claimed that the disks contained a comprehensive survey that would help determine a patient’s risk of contracting the AIDS virus, but each disk contained a virus of its own.

The digital virus was programmed to remain hidden on the host computer for 89 boot procedures. On the 90th, the program would encrypt the filenames on the computer and a message would appear demanding a “license fee” from the user to get the files back. Ransomware was born.

The Virus Has Spread

After that early (and largely failed) attempt at ransomware some 30 years ago, the malware variant went dormant for more than 15 years. Unfortunately, it re-emerged in 2005 and has since gained astonishing momentum.

Ransomware attackers have taken aim at a wide variety of targets, from individual consumers to massive corporations. According to Verizon’s 2018 Data Breach Report, ransomware is to blame for 85 percent of successful attacks against healthcare organizations—attacks which Ponemon Institute research estimated cost these companies a combined $6.2 billion in 2016.

In recent years, ransomware purveyors have also targeted cities and other local governments. The year 2018 saw an attack on Atlanta, Georgia that took more than a third of the city’s 424 different software programs offline, including those necessary for paying bills, running the court system, and providing important information to law enforcement officers.

Atlanta declined to pay the $50,000 ransom demanded by the attackers, and total recovery costs could eventually reach more than $17 million, according to the Atlanta Journal-Constitution. Baltimore faced a similar situation in 2019 and opted against paying an $80,000 ransom. Refusal is laudable, but it’s generally the exception to the rule. When three Florida cities were breached, they paid ransoms that together amounted to $1,460,000 for the chance to recover their systems and continue functions with the least possible delay.

These payouts are the reason the ransomware threat will never disappear—it works, and criminals are pulling in massive profits.

Unfortunately, organizations that pay ransoms are likely just buying time until the next breach. According to The Washington Post, more than 200 U.S. state and local governments fell victim to ransomware in the last few years. In the UK, local authorities are fending off an average of 800 attacks per hour, and the criminals only need to be successful once to do what’s often irreparable damage. Overall, the general criminal consensus is that it works, and they will continue ransoming data because government and industry have done little to stop it.

What’s Behind the Boom?

Partly thanks to the anonymous online payment revolution sparked by Bitcoin, ransomware has become one of the easiest ways for cybercriminals to rake in a profit. For starters, it doesn’t require hackers to infiltrate systems with stealth and then wait for the proper moment to strike. Instead, attacks are conducted rapidly by encrypting files, at which point the attacker simply exposes the hack and demands payment in full view of the user.

Whereas criminals stealing data such as user credentials must then sell that information on the dark web, ransomware shortens the cyberbreach lifecycle by going straight from attack to cash. This payment method also allows criminals to target companies whose data is only valuable to the organization itself. For example, while a criminal on the dark web doesn’t care about the family vacation photos you have stored on Flickr or SmugMug, those corporations (and their users) most definitely do, and they would be devastated to lose control of this data without a backup. In addition to a horde of angry customers, companies that fumble data violate rules established by the General Data Protection Regulation (GDPR) in Europe, and a host of other regional regulations such as the California Consumer Privacy Act (CCPA) in the U.S. As a result, victims are forking over huge amounts of money and criminals are doubling down their efforts.

According to Michael Christman, a section chief of the FBI’s Cyber Division, “I’m aware of one ransomware variant that affected all 50 states that had some $30 million in losses, and over $6 million in ransom payments. I would tell you that the losses are very significant, and easily approach a hundred million dollars or more just in the United States.”

All those payments have added up to make ransomware a booming industry, and McAfee reports that the number of different strains of the malware increased by 118 percent in the first quarter of 2019 alone.¹⁰ Christiaan Beek, McAfee lead scientist and senior principal engineer, points out that “the first quarter of 2019 was game on again for ransomware, with code innovations and a new, much more targeted approach. Paying ransoms supports cybercriminal businesses and perpetuates attacks.”¹¹ Unfortunately, many victims have little choice, and the ransomware industry continues to mature at an alarming rate.

**The Expanding Cybercrime Enterprise and Ransomware-as-a-Service (RaaS)**

With so much funding from paid ransoms, cybercriminal enterprises are achieving unprecedented levels of sophistication and organization. In particular, the rise of Ransomware-as-a-Service (RaaS) has allowed criminals with no technical abilities to lease access to powerful ransomware resources in exchange for sending a portion of each ransom to the malware’s programmers. In a demonstration for CBS’s 60 Minutes, a security expert went to a website offering RaaS and used it to purchase the product and encrypt the contents of one of his own networks. The process took just over five minutes and required zero knowledge of computer programming.¹²

Now, ransomware groups are building and marketing their brands, complete with professional touches such as a public relations presence, customer service chat rooms, and dashboards that keep attackers up to date on the status of their attacks. Ransomware used to be the exclusive domain of skilled hackers and nation-state threat groups.

By eliminating the technical barriers to entry that kept the average criminal from participating, RaaS providers have enabled a new wave of cybercrime that’s sweeping the globe.

**Avenues of Attack**

Attackers have myriad ways of getting past your organization’s defenses, from the most basic phishing email to a hack of your remote desktop protocol (RDP) tool. Stolen RDP credentials are easy to come by on the dark web, and they’re often sold for as little as $20 each.¹³ Criminals also take aim at managed service providers (MSPs) in order to hack a whole roster of client companies with just one successful breach.

Obviously, every breach comes at a cost, but an attack that lands on your mainframe is a worst-case scenario. All of your organization’s most sensitive data resides on the mainframe, making it a primary target for cybercriminals looking to haul in the largest ransom possible. While the pervasive encryption used on the latest IBM® Z® machines provides a layer of security, it doesn’t protect your data from exfiltration or destruction at the hands of hackers—which could potentially be even more catastrophic.

In an effort to secure systems, many companies start with the security framework recommended by the National Institute of Standards and Technology (NIST). This approach has five steps:

1. **Identify Your Assets**
2. **Protect Your Assets**
3. **Detect Incidents**
4. **Respond with a Plan**
5. **Recover Normal Operations**

Most companies have the systems and processes in place to Identify Assets, Protect Assets, and Recover Normal Operations, but they lack the ability for proactive intervention—the Detect and Respond capabilities on the mainframe.

Fortunately, BMC AMI for Security can help protect your data on the mainframe, both by detecting threats and responding to them with automated mainframe intelligence. We’ll start by looking at the keys to early detection that will help you stop incoming attacks before they escalate.

1. **Indicators of Compromise**
   
   When hackers are attempting to force their way into your systems, they can’t avoid leaving behind small pieces of digital evidence. These breadcrumbs might include suspicious logins, unusual port traffic, or system file changes—but they’re only useful if you can spot them in time. Across all attacks in 2018, the average “breakout time” was around four and a half hours, with the fastest threat actors conducting an intrusion in mere minutes. Unless you’re continuously monitoring for Indicators of Compromise, you’re relying on luck to thwart these attacks and avoid being the next ransomware victim. For a more complete list of indicator of compromise, download our whitepaper on the subject.

2. **User Monitoring**

   Privileged user accounts help your most experienced employees accomplish vital functions, but they also pose a serious security threat. According to Forrester Research, 80 percent of breaches involve privileged account access, meaning these users must be closely monitored. BMC AMI for Security helps you bolster your defenses without burdening security personnel by automatically alerting you to anomalous activity, such as a login from an IP address in Czechoslovakia when a user works from an office in Manhattan. You can also receive alerts for a suspicious escalation of account privileges. When a hacker breached the mainframe of a Swedish IT firm, one of his first priorities was escalating privileges of hacked accounts. With escalated privileges, hackers could encrypt the most sensitive datasets on the mainframe and force organizations to pay a potentially crippling ransom.

---

14 https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/
16 https://www.youtube.com/watch?v=SjyjW7qmc&t=1770s
3. **Database Activity Monitoring**
Cybercriminals are always on the attack, which means your approach to defense must be continuous as well. BMC AMI for Security actively monitors databases to ensure you know exactly who is accessing your company’s most vital information, when they accessed it, and what, if anything, they changed. Database Activity Monitoring is also an important part of achieving compliance with cybersecurity regulations depending on the governing bodies in your particular industry and can be the key indicator that a threat actor is attempting to ransom your data.

A collaborative study undertaken by Opus and the Ponemon Institute in 2018 found that 67% of CISOs thought their companies were more susceptible to a cyberattack than in years prior. With the sheer quantity of hackers armed with sophisticated RaaS and chasing rapid payouts, cyberattacks are more of an inevitability than ever before—and yet, 77 percent of organizations lack an appropriate incident response plan.

Two major components of a response plan include:

1. **Incident Response**
When software detects a potentially malicious incident, security analysts must spring into action. By identifying the user ID, IP address, or service that triggered the security alert, they can build a timeline of actions that helps determine if the event was a false positive or an incident that should be escalated. Time is of the essence, particularly with mainframe hardware that could allow threat actors to conduct malicious encryption at lightning speeds. Unfortunately, many organizations realize after the fact that the data they need can be difficult to come by, and without the ability to filter through information, analysts are looking for a needle in a haystack. BMC AMI for Security unlocks a wealth of data on the mainframe by enriching Server Message Facility (SMF) records. With a lightweight agent running on each LPAR, BMC AMI for Security taps into operating system memory and adds important fields before sending information to the security information and event management (SIEM) software or data lake. With details such as user ID, IP address, and more, along with correlation to both mainframe and distributed event logs, analysts are empowered to conduct rapid Incident Response efforts in real time.

---

18 https://www.ibm.com/downloads/cas/GAVGOVNV
2. **Integration with SOC**

If your Security Operations Center (SOC) isn’t providing a clear picture of your enterprise data in addition to other operational security monitoring, it’s not performing its most vital function. BMC AMI for Security integrates seamlessly into all enterprise SIEMs and analytics engines in order to grant your security personnel a complete, 360-degree view of data across both distributed and mainframe systems. With complete visibility and real-time alerting across your entire ecosystem, you can spot threats such as ransomware that often hit multiple systems simultaneously.

Thanks to the immediate payout for criminals and the ready availability of RaaS, armies of hackers are out to hold your organization hostage. To maximize their profit, they’re taking aim at the data stored on your most valuable IT asset—the mainframe.

---

**For more information**

To learn more about how BMC AMI for Security can unburden critical cybersecurity personnel while protecting your mission-critical mainframe, please visit our product page or reach out to a BMC expert today.