Indicators of Compromise and Why It Takes Six-Plus Months to ID a Breach
Table of Contents

03 Introduction

04 Innovation (and Negligence!) has Created Big Business for Cybercriminals Worldwide

05 Indicators of Compromise Vs. Indicators of Attack – What to Watch For

08 Correlate and Alert in Real-Time Across Your Entire Enterprise
Introduction

Poorly Identifying Indicators of Cyberattack Is Why It Takes Us Six-Plus Months to Identify a Breach, and Even Longer to Remediate

Across the U.S., both public and private entities are under assault. Cyberattacks are invisible, but the effects have increasingly been thrust into the limelight, and ransomware is one of the most prevalent threats. In August 2019,¹ The New York Times reported that upwards of 40 municipalities had fallen victim to the data “kidnapping” malware variant. These municipalities range from towns of less than 5,000 to major city centers, including Baltimore and Atlanta. For cybercriminals, they all represent the potential for a massive payday at the expense of taxpayers.

Despite warnings from agencies like the FBI, some local governments are choosing to pay ransoms to hackers in the hopes of getting their files returned and systems fully restored. Not surprisingly, data ransom prices have increased as criminals continue to have their demands met. In March 2019, Jackson County, FL paid out a $400,000 demand. Riviera Beach, a city of 35,000, paid a ransom of $600,000 just three months later. When Lake City was hit, the insurance provider paid hackers $460,000 – a hefty price for a city of just 12,000.

Although it’s easy to see how paying ransoms perpetuates the cycle of cyberattacks, public entities often have little choice when vital systems like emergency response services are down. Steve Parks, a member of the National Cybersecurity & Communications Integration Center’s (NCCIC) Threat Analysis Branch (TAB), explains that “It’s a really tough decision for an organization to have to make, paying the ransom or paying the cost to fix everything once they’ve been compromised. The cost of the latter increases significantly if the organization hasn’t followed industry best practices,”² which means the companies most likely to be breached are also most likely to need to pay up. When systems in Atlanta were breached in 2018, city officials took a stand and staunchly refused to pay a $51,000 ransom. Recovery costs have surpassed $7 million and are still rising as of this writing.³ Information security expenditures are at an all-time high, but hackers continue to find ways to circumvent security controls, predominantly through insider threats and employee negligence.

Hackers will always find novel ways to bypass your security protocols, and fighting cybercrime has become less about prevention and more about stemming the bleeding. Ideally, if you can spot these indicators of attack, you can transform your organization’s approach to data protection from reactive to proactive.

² https://www.youtube.com/watch?v=D8kC07tu27A
³ https://www.theatlantavoice.com/articles/mayor-testifies-before-u-s-house-subcommittee/
Innovation (and Negligence!) Has Created Big Business for Cybercriminals Worldwide

According to Tim Slaybaugh, Malware Analyst at the NCCIC, “For many ransomware authors, developing malware is a business. They’re continuously upgrading and repackaging their tools to make them harder to detect and more effective at compromising systems in an effort to provide a superior product for their clients.” In return for offering their malware as a service, these black hat developers rake in a hefty cut of each successfully conducted attack. Unfortunately, the bad guys just need to be right once, while the good guys must try and maintain secure defenses 24x7x365 in a constantly shifting landscape.

It should come as no surprise that the battle is taking its toll. According to data from CyberSeek, the U.S. alone has more than 300,000 vacant cybersecurity positions – nearly half the total employed cybersecurity workforce of 700,000. Not surprisingly, these unfilled positions put an immense amount of pressure on the individuals who are forced to pick up the slack, and research from the Information Systems Security Association (ISSA) reports that 40% of cybersecurity executives blame the skills gap for high turnover rates and employee burnout. Data from a Spiceworks survey shows that IT professionals are clocking a 52-hour work week on average, with almost 20% exceeding 60-hour weeks. It’s no wonder filling this human resource gap was at the top of CxO priorities in 2019, second only to security.

To make matters worse, a gap in communications between mainframers and the distributed personnel who hold watch over security information and event management (SIEM) systems leads to a consequential gap in security that is more than big enough for a sophisticated hacker to exploit. Even though mainframes power the enterprise computing needs of regulated industries like banking, finance, healthcare, and government, InfoSec resources continue to miss the critical vital signs – indicators of compromise – that spell trouble for highly sensitive data and intellectual property residing on their mainframes.

 Plenty of mistaken assumptions plague mainframe security. Some personnel think that data security standards don’t apply to mainframes, or that mainframes can’t be hacked. Others might not realize that nightly processing of mainframe log data is the fastest way their mainframe can send user events to the distributed SIEM system managing their organization’s cybersecurity. Unfortunately, in today’s threatscape, security measures lacking real-time indicators are creating a security blind spot that, on average, isn’t discovered for more than six months.

---

4 https://www.youtube.com/watch?v=DBkC07tu27A
5 300,000 vacant cybersecurity positions
6 https://www.issa.org/page/2017_isaesg_surv
7 http://www.itmanagerdaily.com/survey-it-pros-are-seriously-overworked/
9 279 days to identify a breach according to 2019 IBM/Ponemon study
Indicators of Compromise Vs. Indicators of Attack – What to Watch for

Around the globe, organizations rely on user log data as the foundation of their security efforts. This data, which can quickly grow to terabytes in seconds in a large enterprise, is indeed an important component of security, but it is not in itself a defense mechanism. Instead, log data empowers an organization to correlate user logs with systems logs (time, user location, system location, access type, etc.) to determine potential anomalies in user activity synonymous with cyber threat. All organizations collect log data, but without combining logs with these other data points – the correlation – they are missing the security events that could be indicators of compromise (IOCs).

IOCs are an important ingredient for your organization's cyber defense, but their presence often means the breach has already occurred. They're largely forensic, used after the fact to compile evidence of a breach and uncover information about the criminal actors involved and the methods they used. Knowing how a system was breached is a great way to ensure that the same method can't be utilized again as soon as your systems are back up and running, but it's still a reactive approach to cybersecurity and one that's costing organizations a fortune.

Instead of relying on traditional IOCs (post-breach indicators), your organization must move from a reactive approach to a proactive one that looks for a different kind of evidence – indicators of attack (IOAs). At BMC, we work with leading penetration testers and build our correlation threads around their tactics, techniques, and procedures. If you are going to proactively mitigate the risk of cyberattack, you’ll need to identify and react to these IOAs in real time. Without a cutting-edge security solution, it's highly possible that an IOA in your organization would have no connection to any malware definition in your security operations center (SOC).

How then, can you leverage both IOC events and IOA events to predict and deter cyber risk? Three key components will help tremendously:

1. Event correlation across both mainframe and distributed systems

2. Visibility of enterprise-wide event data in your organization’s SOC, and

3. Real-time alerts to appropriate personnel (or automation queue) of the impending cyber risk so proactive measures can be undertaken prior to breach

This is immensely easier written here than executed in your enterprise network, but it’s a vital effort if you want to avoid becoming a datapoint in the next major breach report. To create a proactive posture and secure your systemwide data and intellectual property, look for these breach markers that indicate cyber risk:
1. **Port scanning**
   If a source IP is thoroughly scanning your ports, it may be an attacker looking for the best avenues of attack. Instead of blocking the source address, which will just prompt the attacker to use a different one, make sure that the activity isn't sending actionable information back to the cyber criminals – or requesting it from them as part of a command and control process. In some cases, scanning activity might be originating from a partner organization’s network (as was the case in the Target breach of 2013), in which case you should notify their security or network management staff.

2. **Password attacks**
   Repeated failed password attempts could indicate a credential stuffing attack, where an attacker is trying known username and password combinations stolen or bought off the dark web. According to Stacey Wright, Director of Cyber Intelligence at the Multi-State Information Sharing and Analysis Center (MS-ISAC), “If you’re logging these failed password attempts and you have flags set so you get notified when accounts are locked out, that can be extremely effective in detecting a brute force password attack.” Put controls in place that lock out accounts after three to five incorrect login attempts. Even if accounts are only locked for 15 minutes, the measure can drastically slow down the speed at which brute force attacks can be carried out.

3. **Anomalous activity of privileged users**
   Privileged users are an undeniable security risk, particularly on mainframe systems. They have the keys to your most valuable IT asset, and they can wipe their trails clean to make manual detection incredibly difficult. A privileged user accessing a load library s/he doesn’t normally access is not unusual. But, if the access comes from an IP address in Turkey when you know that user always works from their office in the U.S., that’s anomalous activity. Understanding what privileged users are doing in correlation with where they are doing it is critical to your data security. And, with a solution that delivers this information from this critical endpoint device in real-time, you can spot this anomalous activity and even privileged user attempts to erase the activity. More importantly, you can commence remediation immediately and have a forensic record of it.

4. **Escalation of user privilege**
   In the hack of Logica’s mainframe, Gottfrid Svartholm stole credentials for all 120,000 user accounts, including those with administrator privileges. Instead of stopping there, he escalated the privileges of many non-admin users in order to create backdoors once administrators caught wind of the hack and updated their compromised accounts. Secure systems should automatically flag privilege escalation across your user base and notify administrators who can look into the event to confirm its legitimacy.

10 https://www.youtube.com/watch?v=D8kC07tu27A&t=1753s  
11 https://www.youtube.com/watch?v=SjtyifWTqmc&t=1805s
5. **Correlation of user activity to geographic location**
   In the rare event that all of your employees work on-site, you can block IP addresses outside your location and prevent them from accessing your system. If that level of granularity isn’t possible and you have employees telecommuting from around the world, you can still correlate user activity and location to determine when attacks are being conducted. If one of your employees regularly logs into your system from Germany, your system should automatically flag that employee’s attempted login from halfway around the world when you know they were in your Germany office today. Then further investigation or remediation can commence.

6. **Incidence of probing**
   Hackers can gather huge amounts of information by probing your networks, and they’ll use this preliminary research to identify the most promising vulnerabilities in your system. This probing could occur over weeks or months just to understand your organization’s cybersecurity maturity. Besides scanning for open ports, they’ll look for items on your network like user accounts, shared folders, and even connected printers/fax machines, or point-of-sale systems as in the case of the Target breach of 2013. These items are all possible entry points for a hacker to load viruses, key loggers, or other malicious programs.

7. **File integrity monitoring (FIM)**
   Provided you know what your systems look like when healthy, file integrity monitoring lets you compare your current system to that established baseline. It’s a powerful way to monitor changes to the known secure state of your operating systems. Some file integrity monitoring solutions require periodic scans, but an automated solution can give you an accurate picture of changes as they occur in real-time. Even if there is no sign of change to your OS’s file integrity, a simple timestamp change to a file or folder might indicate cyber intrusion. Most FIM solutions are made for distributed systems, but you can do FIM on the mainframe with select vendors, BMC being one of those. Armed with real-time mainframe FIM information, your security teams can spot and stop 0-day threats as they emerge.

8. **Virus definition management**
   It’s imperative that security tools keep an updated database of the latest known virus definitions. A virus such as Mimikatz, for example, allows hackers to steal credentials and escalate privileges on Windows systems, and it’s constantly being updated and improved. ELV.APF is a well-documented open-source tool that performs a similar function on the mainframe. To add an extra layer of protection against these and other threats, software should automatically notify security personnel of any unauthorized changes to virus definitions, as this activity could indicate the presence of a sophisticated hacker.
Correlate and Alert in Real-Time Across Your Entire Enterprise

Cyber criminals and the tools they use are on the offensive 24x7x365. Your approach to proactively securing your data and IP should be an endless, ongoing effort as well. With BMC AMI for Security, BMC's solution built on automated mainframe intelligence, security teams can identify and correlate IOCs and IOAs as they materialize. And they don't have to stare at a dashboard all day. These “breach markers” that appear in your SIEM and SOC can also trigger SMS, email alerts, or other preferred methods of notification to the appropriate security personnel (or system of automated breach response).

BMC AMI for Security is not just security software. It is endpoint detection and response technology coded by security practitioners using a holistic method for data protection built with security solution workflows, automation, high-speed indexing, massive log throughput, and real-time alerts. It is designed as a standalone system, but there is deep integration built into a multitude of complementary SIEM products, and it has the capability to integrate to any SOC. A single system in your technology stack is not going to stop the sophistication and coordination that hackers employ to get to the data they want. Your people and systems need to come together in a united front to quickly spot the indicators that tell you an attack is imminent.

Security functions used to be hidden away in the IT department, but that perception is thankfully evolving. Today, cybersecurity is an integral part of an organization’s IT DNA, and it’s up to CxOs (not just the CISO) to bring known best practices into the spotlight while implementing security solutions that automatically scan for indicators of attack in real-time.

BMC AMI for Security is a solution specifically engineered to protect the mainframe—your most mission-critical IT asset—while removing unnecessary burdens from the shoulders of your overworked IT personnel and augmenting their efforts in powerful ways.

For more information
To learn more about BMC AMI for Security, please visit our product page or reach out to a BMC expert today.

About BMC
BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent

www.bmc.com