BlackBerry
Intelligent Security. Everywhere.

White Paper

Ransomware Prevention Is Possible

Introduction

Ransomware is a form of malware that encrypts files to prevent victims from accessing their systems and data. In almost every case, the files can only be recovered by restoring backup copies, or by purchasing a decryption key from the ransomware threat actor. If the victim doesn't respond promptly enough to the ransom demand, the attacker may increase the ransom amount or delete the decryption key, rendering the files impossible to retrieve.

Although law enforcement advises victims not to accede to ransom demands, many firms will pay anyway based on the degree to which their operations are impaired, the potential impact on customers and shareholders, the relative costs of recovery and cleanup, and the extent to which exposure could subject them to regulatory penalties or damage their brand or reputation.

Today, ransomware is big business for nation-state actors and cyber-criminal organizations alike, accounting for 27%[1] of all malware-related security incidents. Consider these troubling statistics:

- There will be a ransomware attack on businesses every 11 seconds by the end of 2021[2]. Every 40 seconds, one of those attacks will prove successful[3].
- 62% of the organizations responding to a 2020 Cyberthreat Defense Report[4] said they had been victimized by ransomware. 58% of those firms opted to pay the ransom, an increase of 13% over the year before.

Ransomware As a Cyber Weapon

In the BlackBerry Cylance 2020 Threat Report, the BlackBerry Research and Intelligence Unit noted a number of key trends emerging in the ways that threat actors conduct their ransomware campaigns. Chief among them is the use of ransomware in highly targeted attacks, such as those utilizing the Sodinokibi, Ryuk, and Zeppelin[5] ransomware families.

This trend first gained widespread public attention with the outbreak of WannaCry (2017)[6]. After a brief period of decline, ransomware came back with a vengeance. Traditionally, ransomware attacks were financially motivated cyber crimes directed at individual users and small or midsize businesses. More recently, however, BlackBerry's Research and Intelligence Unit has observed a substantial increase in cases of big companies, public institutions, and governments being hit by ransomware.

In some of the most sophisticated scenarios, attackers will choose their victims carefully and do a thorough reconnaissance to find the best way in. Once they gain access to the victim's environment, the attackers first deploy information-stealing

1 Verizon 2020 Data Breach Investigations Report
2 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
3 What It Means To Have A Culture Of Cybersecurity
4 2020 Cyberthreat Defense Report
5 BlackBerry 2020 Threat Report,
6 WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

malware and exfiltrate sensitive data before encrypting files[7]. If the affected company refuses to pay for the decryption tool, the attackers will try to blackmail them with a threat of publishing the stolen information. This often contains personal data of the company's customers and would therefore constitute a data privacy breach. Approximately 10% of the attacks detected by or responded to by BlackBerry® security products and services have utilized this tactic[8]. The Maze ransomware group is a recent example[9].

While phishing remains the most common attack vector, threat actors also utilize tactics, techniques, and procedures (TTPs) that don't require a victim to click on a malicious link or open a weaponized document to become infected. The BlackBerry® Security Services Incident Response team, for example, has noted multiple instances of attackers compromising VPNs running deprecated software. Others are utilizing fileless exploits, such as Cobalt Strike, to take control of a vulnerable system by injecting malicious code into a running process. Memory-based attacks like these are designed to defeat traditional antivirus products that rely on file signature matching and heuristics techniques to protect endpoints.

Once accomplished, the attacker can install a backdoor connection to a command and control (C2) server, modify the system registry to maintain persistence, and load tools that aid in network reconnaissance, credential theft, and lateral movement. Only after all targets of interest have been identified and compromised will the ransomware be deployed and detonated.

Threat actors behind targeted ransomware attacks tend to reuse known malware families. Many of these are sold on underground forums or bought from ransomware-as-a-service (RaaS) vendors. Most often, the aim is extortion. However, some ransomware attacks are designed to disrupt processes and services by destroying vital data or utilize a flawed payment infrastructure and/or encryption routines that make file decryption or ransom payments impossible.

Anatomy of a Sophisticated Ransomware Attack

First discovered in August 2018[10], Ryuk is a strain of ransomware associated with a notorious Russian cyber-criminal group that, according to the Federal Bureau of Investigation[11], extracted more than $61 million in bitcoin payments from victims between February 2018 and October 2019[12].

Ryuk has also been flagged as a global threat in a June 2019 National Cyber Security Centre (NCSC) advisory[13]. The authors note that after gaining access, the group often spends anywhere from days to months conducting reconnaissance before depositing and detonating Ryuk. In some cases, however, Ryuk attacks proceed

7 Another ransomware strain is now stealing data before encrypting it
8 Threat Bulletin: Ransomware 2020 – State of Play
9 Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up
10 CISA Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector
11 Ransomware victims are paying out millions a month. One particular version has cost them the most
12 RSA Presentation: Feds Fighting Ransomware: How the FBI Investigates and How You Can Help
13 Ryuk ransomware targeting organisations globally

much more quickly. One high profile example is the recent attack on Universal Health Services (UHS), a Fortune 500 provider of hospital and healthcare services that treats approximately 3.5 million patients each year.

The attack was first reported by Bleeping Computer[14] on September 28, 2020. Within five hours of the initial infection, hundreds of the firm's healthcare facilities across the United States, including those in California, Florida, Texas, Arizona, and Washington D.C., lost access to their computer and phone systems. As a result, UHS employees were forced to delay patient appointments and, in some cases, reroute emergency room patients to alternate facilities[15].

In the aftermath of the attack, analysts at the DFIR Report[16] reconstructed the kill-chain as follows:

1. The initial infection was the result of a phishing exploit that deposited BazarLoader malware onto the victim's computer. Developed by the TrickBot group[17], Bazar is a trojan that utilizes code signing certificates and a variety of obfuscation techniques to avoid detection[18].
2. Once installed, the malware created a backdoor connection to the threat actor's C2 server, and began mapping the UHS network using legitimate Windows utilities such as Nltest[19], a Microsoft Windows Server command line tool that generates lists of domain servers.
3. After locating UHS's primary domain server, the attackers acquired administrator privileges with Zerologon, a privilege escalation vulnerability found in selected Microsoft Windows Server operating systems that is rated as critical (a score of 10.0) in the Common Vulnerability Scoring System[20].
4. Next, the Ryuk group utilized Server Message Block (SMB) file transfers and Window Management Instrumentation (WMI) executions to deploy the Cobalt Strike toolkit. This enabled them to locate and then move laterally to the secondary domain controller, where they continued conducting domain discovery with PowerShell Active Directory scripts.
5. Now, having identified their domain server and data store targets, the attackers utilized the same techniques to acquire administrator control over the secondary domain server.
6. Having completed their reconnaissance and targeting, the attackers utilized RDP to deposit the Ryuk executable on the primary DNS server, network storage devices, and employee workstations. The final step was to execute the Ryuk ransomware.

---

14 UHS hospitals hit by reported country-wide Ryuk ransomware attack
15 A Ransomware Attack Has Struck a Major US Hospital Chain
16 Ryuk in 5 Hours
17 BazarBackdoor: TrickBot gang's new stealthy network-hacking malware
18 Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon
19 Microsoft command line reference
20 NIST National Vulnerability Database CVE-2020-1472 Detail

What Should Security-Minded Enterprises Do?

Let's start with what savvy security-minded organizations should not do; namely, adding yet another security layer to what may already be an overly complex and unmanageable security infrastructure. An excessive number of security controls can have the unintended effect of reducing, rather than enhancing, an organization's cyber resilience. According to an IBM Security report[21], nearly 30% of the organizations surveyed have 50 or more security tools deployed. Compared to peers with fewer tools, these organizations ranked 8% lower in their ability to detect attacks and 7% lower in their capabilities for incident response (IR).

Partly, this is due to alert fatigue, and partly, a consequence of the huge volumes of telemetry and event data generated by endpoints and other networked devices. How is an analyst to efficiently comb through this data to detect the subtle signal of a threat from the random noise of routine activity?

Thus, new investments should wait until the business and security leadership teams have acquired a thorough understanding of the organization's cyber-risk exposure and risk tolerance.

Begin with Planning and Assessments

BlackBerry experts often recommend that a client begin with a Compromise Assessment (CA) engagement. This helps to identify risk factors and establish a baseline for evaluating future security upgrades. A CA should address the twin domains of threat hunting and attack surface reduction, with a focus on:

- Data exfiltration and sabotage
- Command and control activities
- User account anomalies
- Malware and persistence mechanisms
- Vulnerable network, host, and application configurations

The CA findings and recommendations should be reviewed with the client's security and business leadership teams.

- **Threat Hunting Findings:** If a past or current compromise is detected, the nature, extent, and impacts on the environment should be detailed.
- **Attack Surface Reduction Findings:** These should include both strategic and tactical recommendations for improving the organization's overall security posture, along with a risk-prioritized assessment of attack surface reduction opportunities. For example, the CA should flag systems with critical vulnerabilities, such as Zerologon, and provide step-by-step instructions for ameliorating them.

21 Cyber Resilient Organization Report 2020

According to IBM[22], the "vast majority" of organizations today are unprepared to respond effectively to a serious security incident. And in a 2020 survey[23], IBM found that it took an average of 315 days for organizations to identify and contain a data breach caused by a malicious attack. Reducing that response time is essential for operational resilience. It also benefits the bottom line. Organizations that resolve incidents in less than 200 days realize average costs savings of $1.12 million[24] compared to those who take longer.

To address these concerns, BlackBerry recommends that clients formally assess their defensive team's capabilities for identifying, containing, eradicating, and recovering from a security breach. The investigative process should encompass staff interviews, a security policy gap analysis, and an evaluation of the defensive team's performance during a customized incident response (IR) exercise. Based on these findings, the IR plan should be revisited to ensure it conforms to industry best practices and regulatory standards.

Assessments like these are important, but they are no substitute for testing a defensive team's capabilities in an authentic, real-world attack scenario. BlackBerry Security Services, for example, offers both Breach Simulation and Adversary Simulation engagements to meet varying client needs. Breach Simulations are a good fit for organizations that want to exercise their defensive capabilities, validate their security assumptions, and identify gaps in their security posture. Adversary Simulations are a good fit for organizations that want to acquire experience in detecting and responding to attacks by real-world threat actor groups that are actively targeting their industry.

For more information about the BlackBerry Security Services portfolio, visit our website.

Preventing Ransomware Incidents with BlackBerry Protect

The most efficient way to prevent a ransomware incident from occurring is to stop an attacker from exploiting a system vulnerability with a malicious script or utilizing malware to deposit ransomware on a victim's computer. BlackBerry® Protect is an endpoint protection platform (EPP) solution that utilizes sophisticated artificial intelligence (AI) and machine learning (ML) technology to stop both tactics.

Deployed at the endpoint utilizing BlackBerry unified agile agent technology, BlackBerry Protect determines in milliseconds whether a file is safe to run. If so, the file is permitted to execute. If not, execution is prevented, the file is quarantined, and a set of alert and contextual data is displayed in the BlackBerry® Cyber Suite management console. This file detection process is performed independently on each endpoint and consumes minimal system resources. There is no need to consult a remote database, install continual updates, or connect to the cloud. BlackBerry Protect AI models detect and prevent the execution of malware and ransomware in both open and isolated networks.

---

22 IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them
23 IBM Security Cost of a Data Breach Report 2020
24 IBM Security Cost of a Data Breach Report 2020

In addition to preventing malicious files from executing, BlackBerry Protect prevents threat actors from injecting and executing malicious code in system memory by monitoring all 32- and 64-bit running processes for behaviors associated with common exploits. If a memory violation is detected, BlackBerry Protect intercepts the resulting function call so that corrective actions can be taken before the function is allowed to execute. These range from ignoring the violation and allowing execution to terminating the process completely. These capabilities prevent threat actors from utilizing malware, such as Bazar, to highjack legitimate system services to pursue their objectives.

BlackBerry Protect also prevents the execution of malicious PowerShell, Active Scripts, and Microsoft Office Macro scripts like those used by the UHS threat actors. Typically, Script Control policies are initially set to Alert Mode, so that administrators can determine which scripts are being used, who is using them, and whether and under what conditions they should be allowed to run. Once the inventory is complete, Block Mode can be enabled, thereby preventing all scripts from running except those installed in specified folders or explicitly named in exclusion rules.

Ransomware can also be introduced into a network via a compromised mass storage device. BlackBerry Protect Device Control policies minimize such risks by preventing employees from installing unauthorized software, exfiltrating data, or inadvertently compromising business systems with infected devices. BlackBerry Protect Device Control policies apply only to mass storage devices. Peripheral devices, such as mice and keyboards, are not affected.

BlackBerry Protect Application Control enables organizations to continuously maintain the pristine state of their fixed-function devices by preventing threat actors from installing malware or modifying the operating system, firmware, network stack, and supporting applications.

Ransomware Threat Hunting, Remediation, and Recovery with BlackBerry Optics

If BlackBerry Protect is so effective at stopping ransomware attacks, then why is an endpoint detection and response (EDR) solution like BlackBerry® Optics needed?

First, and most obvious, there is a small, but discernible, difference between 100% efficacy against malware execution and the better than 99% efficacy [25]achieved by BlackBerry Protect. It's simply prudent to have a system in place that can contain and facilitate the investigation of a ransomware attack that gets through one's first line of defense.

The second factor is the changing nature of the threat environment. In its 2020 Data Breach Investigations Report[26], Verizon assessed the tactics used by threat actors, and concluded that, "Malware has been on a consistent and steady decline as a percentage of breaches over the last five years," noting that, "45% of attacks featured hacking, 22% of breaches were caused by errors, 22% included Social attacks, and

25 NSS Labs Advanced Endpoint Protection Cylance Security Value Map, April 2018
26 2020 Data Breach Investigations Report

17% involved Malware." This doesn't mean that malware is fading away as an attack vector, only that adversaries are increasing the utilization of TTPs that don't require the use of portable executables, at least during the initial stages of the kill-chain.

BlackBerry Optics is an EDR solution that extends the threat prevention delivered by BlackBerry Protect by providing true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities. Unlike other EDR products, BlackBerry Optics doesn't require significant investments in on-premises infrastructure or reactive approaches that rely on streaming data continuously to the cloud. Instead, BlackBerry Optics applies detection and response logic at the endpoint, eliminating the response latency that can make the difference between a minor security event and a major uncontrolled security incident.

To detect ransomware threats, BlackBerry Optics incorporates a Context Analysis Engine (CAE) that monitors endpoint events in near real time to identify malicious or suspicious activities. The CAE comes with a prepackaged set of BlackBerry-curated detection logic that can trigger a myriad of responses. This includes rules derived from real-world attacks investigated and resolved in the field by BlackBerry incident response teams as well as attacks deconstructed and documented by BlackBerry threat researchers. For example, BlackBerry's Threat Research Unit has authored custom BlackBerry Optics rules that tag and mitigate against the techniques utilized by Ryuk malware variants[27].

While detection rules are necessary, they cannot model every kind of attack behavior. Therefore, BlackBerry Optics also includes machine learning threat detection modules developed by the BlackBerry Data Science team that continuously analyze endpoint activity to detect zero-day, APTs, and living off the land attacks like those conducted by the most sophisticated ransomware threat groups.

BlackBerry Optics provides for both on-demand and automated responses whenever a CAE rule or machine learning detection is triggered. These include such things as collecting forensic data, taking systems offline, and performing other functions needed to investigate and resolve a ransomware outbreak.`

Once an incident is detected, it must be thoroughly investigated to ensure that all stages of the kill-chain are understood and accounted for during subsequent containment and recovery efforts. BlackBerry Optics includes both manual and automated incident investigation tools that enable analysts to efficiently hunt for threats and perform root cause analysis.

For example, BlackBerry Optics simplifies the threat hunting process by enabling security teams to collect forensically-relevant data via InstaQuery (IQ) searches. IQ is a lightweight tool that can collect data from any endpoint, aggregate the results, and then present them in a format that is both contextualized and intuitive to analyze.

---

27 Ryuk Malware Optics Rules

BlackBerry consultants recently utilized IQ to help a large enterprise investigate and remediate a ransomware outbreak. Within seconds, the team determined that the primary IOC, the ransomware's file extension, was only present in the United States. This enabled the client and BlackBerry teams to focus their investigation, remediation, and cleanup efforts there, rather than spending unproductive hours assessing the client's operating environments in Europe, Asia, and the South Pacific. BlackBerry consultants also assisted the client in preventing further infections by creating and distributing custom rules that ensured the ransomware would be detected instantly and promptly quarantined.

Benefits of BlackBerry's Approach To Preventing Ransomware Incidents

BlackBerry's portfolio of ransomware software and service solutions enable organizations to:

- Prevent ransomware from executing or utilizing legitimate system services to gain a foothold and begin lateral movement.
- Stop ransomware from inflicting damage by deploying automated detection, response, and remediation routines that aid in proactive threat hunting and root cause analysis.
- Respond rapidly to ransomware incidents. The wait time for a mid-tier provider or large consulting firm to respond to a breach can stretch into weeks, allowing damage to spread and driving up the costs of recovery and cleanup. BlackBerry ransomware experts are available at a moment's notice to deliver consistent, best-in-class services.
- Minimize risk exposure by obtaining the expert guidance and support that CISOs and security teams need to identify and close gaps in their security fabric, harden their cyber defenses, implement robust processes for incident response, and transition efficiently from a reactive to a prevention-first security posture.

Parting Thoughts

So, to what extent can we conclude that ransomware incidents really are preventable? That depends a great deal on one's concept of prevention. If you think it means throwing a magic switch that shuts off ransomware attacks, then, no, sadly, you're going to be disappointed. BlackBerry's view, however, is that almost all ransomware attacks can be stopped cold at the delivery stage of the kill-chain if practical steps are taken to defeat them.

That begins with a thorough assessment of computing infrastructure to identify and prioritize cyber risks. Systems with widely known vulnerabilities should be patched to avoid exploitation. The same applies to system configuration errors. For example, external access to RDP systems should be disabled to prevent BlueKeep exploits[28].

Basic blocking and tackling shouldn't be ignored. Employees need ongoing training to resist social engineering attacks. Sub-par password policies should be shored up by implementing multi-factor and continuous authentication technologies. Organizations must also fully commit to ongoing security assessments to determine how emerging threats and digital transformation projects could expose them to new kinds of cyber risks. These initiatives require long-term commitments that yield long-term benefits.

However, there are quick wins that should be taken without delay. BlackBerry Protect detects and stops ransomware as well as the fileless techniques ransomware threat actors use to gain an initial foothold. Artificial intelligence and machine learning make all the difference when it comes to stopping sophisticated attacks. And if an attack does somehow slip through an organization's defenses, BlackBerry Optics steps in, firing off automated response and remediation routines to prevent a security breach from becoming a widespread security incident.

So yes, ransomware prevention is not only possible, but also practical too.

Learn more about BlackBerry's portfolio of ransomware prevention and remediation solutions or call +1-888-808-3119 for immediate assistance.

For additional BlackBerry perspectives on stopping ransomware and resources, visit our website.

---

28 NIST Vulnerability Database CVE-2019-0708

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MKTG 19-0108 | 210115