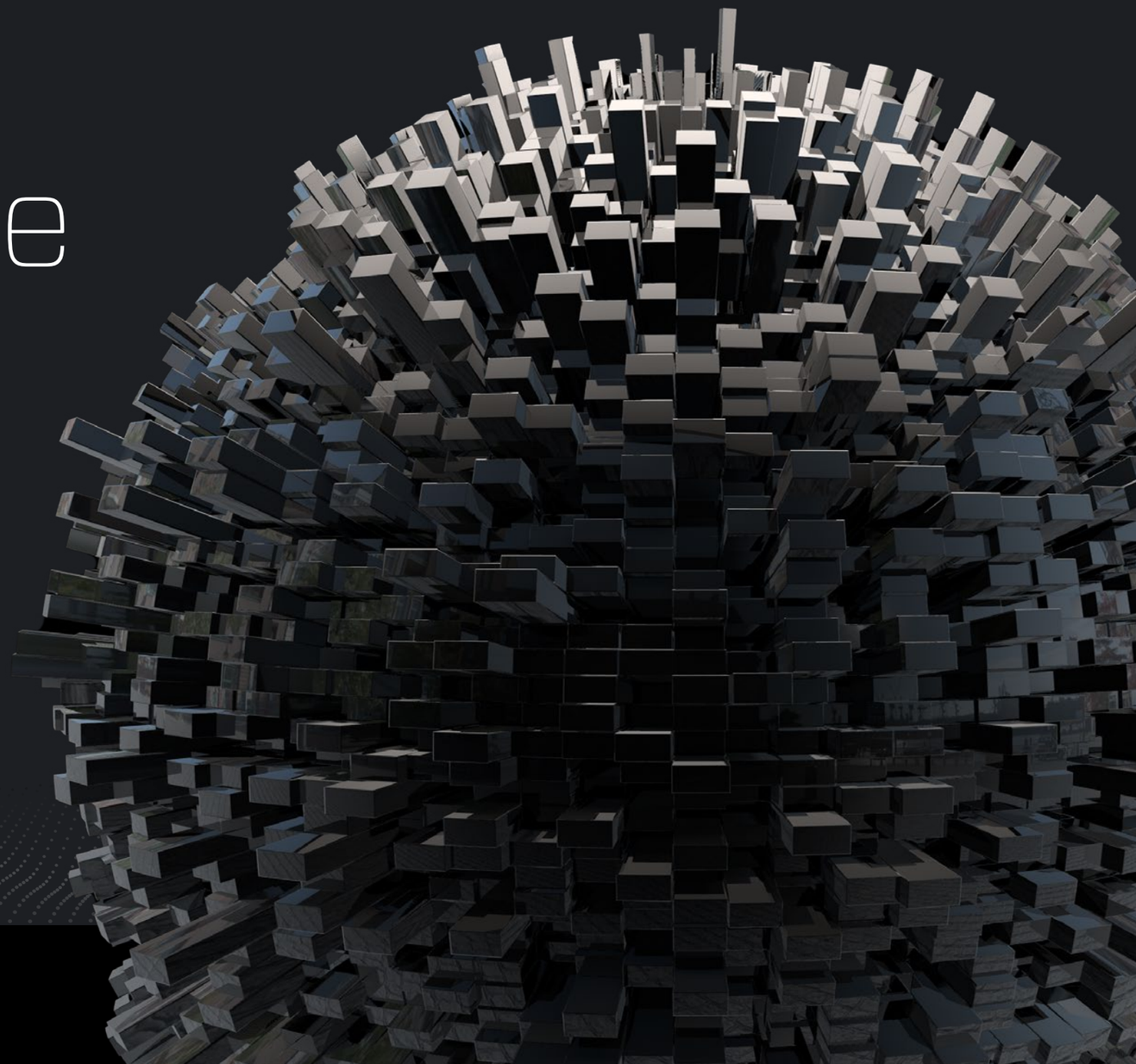
2020

Threat Report Discussion Guide



This guide is intended to highlight major points of interest from the BlackBerry® Cylance® 2020 Threat Report. Our analysis is derived from customer and industry threat data that spans 2019, and is presented for the benefit of security professionals and interested readers. Security teams and managers can use this guide to prioritize the current cyber risks facing their organizations. Understanding recent cybersecurity trends can help security professionals effectively allocate their staff, tools, technology, and related resources against an ever-evolving threat landscape.

BlackBerry | CYLANCE

Host-Dependent Encryption

In 2019, BlackBerry Cylance noted an increase in APT-related malware samples using host-dependent encryption to protect their payloads. In the past, this technique was used to protect the most sensitive, highly tailored backdoors, and usually implemented via Windows® Data Protection APIs. Recently, these encryption mechanisms have become more diverse and widespread. Some threat actors have built host-dependent encryption into their generic loaders which are distributed with a range of various tools and malware.

POINT FOR DISCUSSION

How are you defending your organization from this increasingly utilized technique for deploying malicious payloads?

Increased Data Loss from Misconfigured Cloud Resources

BlackBerry Cylance examined publicly disclosed data breaches in 2019 and observed some interesting trends regarding data leakages caused by cloud misconfigurations. On average, there were at least three disclosures of exposures caused by unsecured databases and servers every month. These data exposures led to a total of over seven billion records being publicly exposed.

POINT FOR DISCUSSION

How is your organization working to proactively balance security measures and manage software-defined infrastructure required to support its evolving business needs?

Read more about best practices for deploying a multi-faceted approach to cloud security here.

Ransomware

After a brief period of decline, ransomware has come back with a vengeance. In the past, ransomware attacks were financially motivated cyber crimes directed at individual users and small or medium-sized businesses. More recently, however, we have 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.

POINT FOR DISCUSSION

What defenses are you using to ensure that no one can gain access to your environment?

The threat actors behind targeted ransomware attacks tend to reuse known malware families. Many of these malware families are sold on underground forums or bought from ransomware-as-a-service (RaaS) vendors. The aim of most of these attacks is often simple extortion. Attackers often exfiltrate sensitive data from an environment before deploying ransomware, and may use it as leverage to coerce the victim to pay. The contents of the stolen data may influence the final ransom price demanded by the threat actors, depending on its sensitivity. Other ransomware attacks may aim to disrupt processes and services by destroying vital data.

POINT FOR DISCUSSION

What is your organization doing to protect itself from falling victim to ransomware attacks? What is the contingency or remediation plan for your organization, should it fall victim to one of these attacks?

Learn more about preventing and remediating ransomware attacks here.

Living Off the Land

In 2019, threat actors continued to rely heavily on living-off-the-land (LotL) techniques which use trusted system resources for cyber attacks without triggering security alerts. Attack vectors vary, but include:

- Using reconnaissance and lateral movement tools like WMI and built-in scripting languages (PowerShell, VBScript, etc.)
- Using administrative and development tools for:
  - Evasion
  - Deploying fileless malware
  - Proxying execution

POINT FOR DISCUSSION

Are you familiar with the indicators of a LotL attack?

What specific defenses have you set up to ensure that you can identify when these types of attacks are occurring within your environment?

Learn more about preventing damage from LotL and fileless attacks here.

Coinminers

With the rise of cryptocurrencies, criminals have recognized a unique opportunity to generate an additional revenue stream on compromised machines. By using a computer's hardware, malicious software can generate crypto coins which are automatically deposited in the attacker's wallet. Coinmining requires minimal work (and technical skill) from the attacker's perspective. Additionally, coinmining malware can passively generate revenue from all infected machines unlike ransomware, which might only see returns from one in 1,000 victims.

POINT FOR DISCUSSION

Are you and your team aware of the indicators of coinmining attacks?

Phishing

Phishing is a technique that relies on social engineering to lure victims into divulging confidential information such as passwords and banking details. The most common way users encounter phishing is through emails containing malicious attachments or links. This method is typically used by financially motivated attackers who are not focused on a specific person or organization. Alternatively, phishing can be fine-tuned to target a single victim using specific details relevant to them. This technique is called spear phishing and is more likely to be used by attackers looking for access to a specific system.

POINT FOR DISCUSSION

Phishing remains a threat today due to the potential of human error. What is your organization doing to protect against the inevitable perils of human error both at home and in the workplace?

Learn more about how you can better protect your organization and your family from phishing attacks here.

Mobile Security

Recent research from BlackBerry Cylance found that state-sponsored advanced persistent threat (APT) groups are exploiting mobile devices with impunity to surveil:

- Specific people of interest
- Traditional foreign intelligence
- Economic espionage targets

As public awareness of these attacks increases, we expect to see significant investments from enterprises and governments in mobile threat detection and response.

POINT FOR DISCUSSION

Is your organization actively discussing increasing its mobile security defenses and detection and response capabilities?

Deep Fakes

There has been a significant increase in the number of deep-fake videos released in 2019. The overall number of deep-fake videos released by December of 2018 was doubled within the first nine months of 2019. There were also three reported real-world cases in which AI-generated audio outputs spoofed CEO voices to trick victims into transferring large sums of money. Deep-fake trends will likely increase in 2020, driven by factors like:

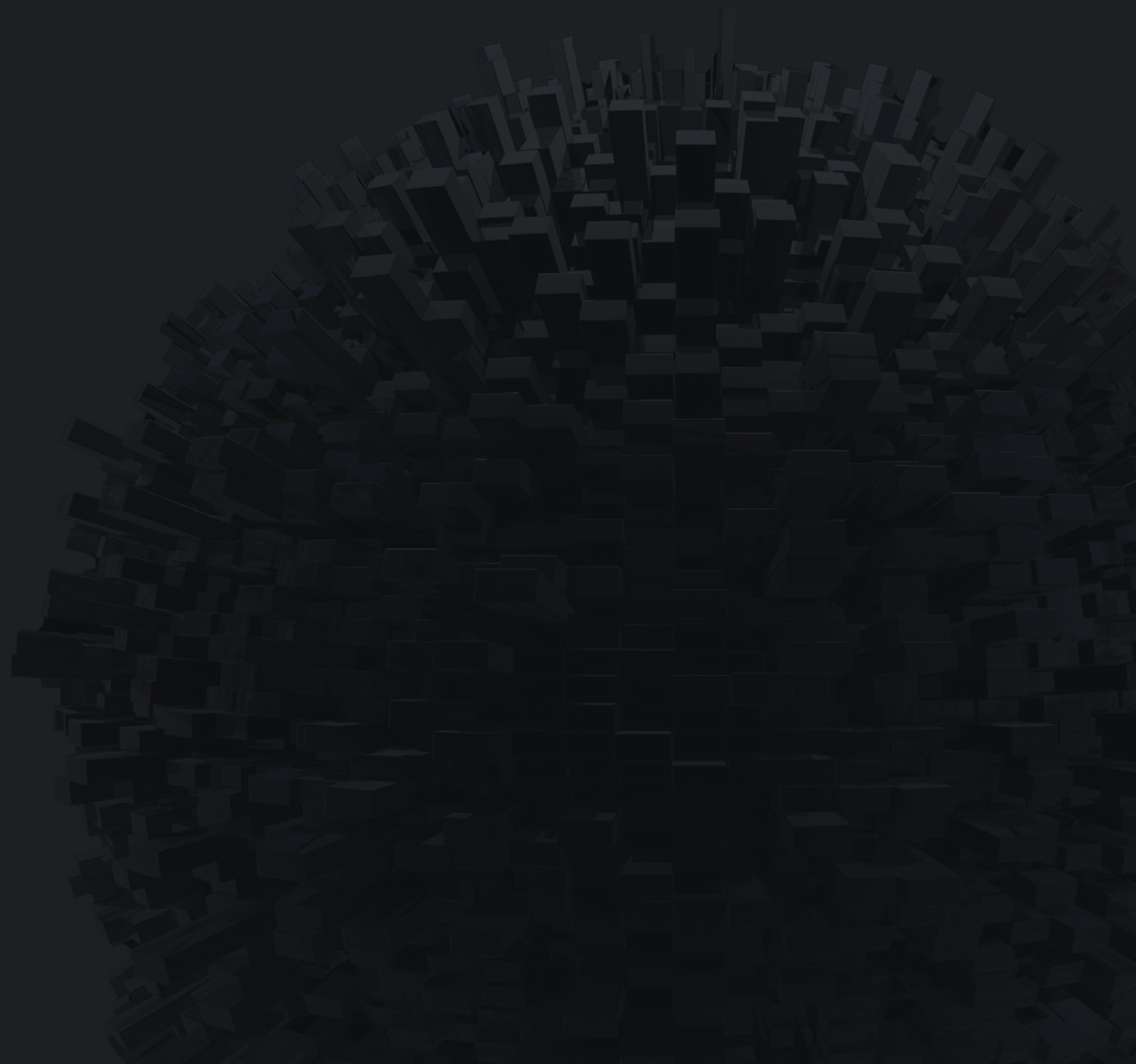
- Disinformation campaigns supporting geopolitical activity
- An increase in the availability and sophistication of tools needed to produce realistic outputs
- The effectiveness of deep fakes as a social engineering tool

Better tools that make deep-fake technology accessible to more users

POINT FOR DISCUSSION

Have you provided any educational training for employees at your organization on identifying deep fakes and how they can be used for fraud?

Get the full report here



BlackBerry | CYLANCE

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 20-0049-20200211