This guide is intended to highlight major points of interest from the BlackBerry® 2021 Threat Report. Our analysis is derived from customer and industry threat data that spans 2020, 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. The report provides information you need to prepare, prevent, detect, and respond to the cyber threats of the upcoming year.
Threat actors adapt quickly to crises, and the COVID-19 pandemic was no exception. As workers transitioned to home offices and businesses struggled to adjust their operations, cyber attacks spiked by 63%\(^1\). Attackers conducted mass phishing campaigns using COVID-19-themed lures and created malicious mobile apps to exploit the fear of citizens worldwide. While the pandemic is the largest crisis in recent memory, threat actors similarly exploited Hurricane Harvey in 2017 and Hurricane Katrina in 2005. The pattern is clear; when disasters disrupt company operations, attackers quickly respond by directly exploiting the situation.

Threat actors are increasingly embracing ransomware-as-a-service (RaaS), which offers attackers vendor support and better results due to frequent updates by the RaaS distributor. Likewise, ransomware targets have shifted from random individuals to larger, more critical organizations, like those in the healthcare industry. There has also been a recent change in ransomware tactics to include data exfiltration and extortion attempts. Attackers have moved from merely threatening catastrophic data loss, to threatening to publish exfiltrated data and damage the victim’s brand. Threatening to publish stolen data results in a greater likelihood of ransomware payment\(^2\).

Increased remote working presented a new opportunity for cyber criminals to launch COVID-19-themed phishing attacks. Data from the Anti-Phishing Working Group shows that the number of phishing campaigns grew since March 2020\(^3\). Software-as-a-service (SaaS) applications and webmail remained the most targeted services for phishing attacks, dominating others throughout the year. BlackBerry researchers also witnessed the use of trojanized applications to steal OAuth access tokens. Dubbed “consent phishing”, these malicious campaigns provide an attacker a means to bypass multi-factor authentication (MFA).

**Point for Discussion**

How can your organization prepare for the inevitable increase in cyber attacks that occur during a time of crisis?

Is your organization prepared to withstand a focused ransomware campaign? How would it react to extortion attempts involving exfiltrated data?

What steps can your organization and employees take to defend against sophisticated phishing attacks?

---

3. [https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf)
**CRYPTOJACKING**

Cryptojacking, the unauthorized use of a computer to mine cryptocurrency, offers an illicit way to work around the rising costs of cryptomining. Cryptojackers often target high-powered servers in an enterprise environment in order to maximize their mining activities. Threat actors have multiple ways to infect devices with cryptojacking malware. Two common attack vectors are malicious links or embedded cryptomining scripts in web pages. Once a machine is infected, the attacker can use it to mine cryptocurrency, often without the knowledge of the legitimate owner.

**OFF-THE-SHELF THREATS**

All cyber attacks are not extremely advanced efforts carried out by an elite group of threat actors. In fact, cyber attacks have been commodified like any other industry where persistent consumer demand drives the creation of simplified off-the-shelf offerings. Last year, unscrupulous attackers used ready-made threat tools and services including exploit kits, malspam campaigns, threat emulation software, and Mimikatz. Other tools, like Adfind and Sharphound, were used by threat groups for information gathering, domain mapping, and lateral movement within an environment.

**MOBILE SECURITY**

Threat actors are exploiting user expectations and vulnerable smartphone overlay services to prey on unsuspecting users. The premise of the attack is simple; present a credential or payment request at a time when a user is interacting with a target application. The sudden prompt will not seem unduly suspicious, and users may quickly re-enter their credentials without giving it much thought. This attack is used by banking and information stealing malware families including Anubis, Ginp, Cerberus, EventBot, and Marcher.

**Point for Discussion**

How does your organization detect and identify cryptojacking attacks, which often operate unnoticed for long periods of time?

**Point for Discussion**

How would your environment detect and respond to the off-the-shelf threats widely used by malicious individuals and groups today?

**Point for Discussion**

Are the smartphones that access your business and personal data protected against overlay attacks?
One of the first cases of deepfake weaponization in the workplace was discovered last year. A senior official was tricked into transferring money after he received a call from a fraudster who impersonated the CEO’s voice using deepfake technology. In Belgium, a deepfake video of the Prime Minister linking the cause of the pandemic to environmental damage was released by climate activists. Creating believable deepfake audio and video no longer requires rare expertise or access to considerable funding. Researchers also discovered several underground forums selling deepfake services with more actors seeking ways to monetize this technology. Perhaps one of the most publicized weaponizations of this technology was centered around supporting disinformation campaigns.

Point for Discussion

What processes are in place to protect and verify the identities of key personnel in your organization, and as normalcy returns, how will you protect against this growing threat?
