WHITEPAPER

Bitdefender

Security

The 'New Normal' State of Cybersecurity

2020 - BUSINESS THREAT LANDSCAPE REPORT

www.bitdefender.com

Contents

"In the wake of 2020, ***50 percent[1] of organizations were unprepared*** *to face a scenario in which they would have to migrate their entire workforce in a work-from-home environment. The global SARS-CoV-2[2] pandemic may have been a respiratory illness that affected people around the world, but it also impaired the way organizations and business conducted normal operations.*

The lack of forward planning for such a scenario left many organizations open to potential vulnerabilities and misconfigurations that threat actors could have easily leveraged to score breaches, exfiltrate data, or even generate additional profit by extorting vulnerable companies.

To help infosec professionals plan ahead their cybersecurity strategy in 2021, Bitdefender is releasing its yearly threat landscape report early this year, as part of the international cybersecurity awareness month.

We trust that this extensive information gathered from our 500 million sensors worldwide will provide businesses with a solid ground to build long-term WFH cybersecurity strategy."

Bogdan Dumitru, CTO at Bitdefender

1 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

2 "Severe acute respiratory syndrome coronavirus 2", Wikipedia, https://en.wikipedia.org/wiki/Severe_acute_respiratory_syndrome_coronavirus_2

Foreword

Key Telemetry Findings

- 93.10 percent of human risk factors involve employees using old passwords for accounts
- 87.31 percent of all misconfigurations involve having WinRM Service enabled
- 46.84 percent of all reported network-level attacks involve SMB exploits
- 41.63 percent of all reported network-level attacks involve bruteforce attempts on RDP and FTP
- 46 percent increase in suspicious IoT incidents in households throughout the first half of 2020
- 4 in 10 emails on the Coronavirus topic are fraud, phishing, or malware
- 63.63 percent of all reported unpatched vulnerabilities involve CVEs that are older than 2018 (inclusively)
- 42.52 percent of Execution stage Command and Scripting interpreter sub-techniques involve the use of PowerShell Commands and Scrips

Key Findings

WORK FROM HOME & PANDEMIC IMPACT. Businesses and organizations of all sizes have shifted their workforce almost overnight in an indefinite work from home scenario, as a result of the Covid-19 outbreak. Network security controls and policies that were in place within the corporate network had to undergo significant changes to accommodate employee devices connecting to the corporate infrastructure from untrusted networks. However, it's IoT devices that 45 percent[3] of CISOs and CIOs fear as being the biggest risk to employee home networks, as they could easily be hacked by threat actors and used to compromise employee devices or even their entire network.

MISCONFIGURATIONS. The new work from home scenario has potentially opened up corporate infrastructure to new attack vectors and threats that they would have never considered a year ago. With most organizations struggling to suddenly accommodate their entire employee workforce as remote, some **security misconfigurations and oversights are bound to have happened**.

One of the most reported misconfigurations, especially since work-from-home became the new normal, involves WinRM Service enabled and poorly configured. Bitdefender business telemetry reports that nine in 10 endpoints seem to repot this as the top misconfiguration, which means that successful exploitation by threat actors could lead to either endpoint compromise or other business infrastructure risks.

INTERNET-OF-THINGS. On top of that, **45 percent** of security professionals also believe that internet of thing (IoT) devices in employee home networks pose serious security risks as they could be easily controlled by remote hackers and compromise corporate infrastructure. In fact, Bitdefender telemetry has shown that the number of s**uspicious IoT incidents in households has increased by 46 percent[4] from January until June**. **Port scanning attacks account for 55.73 percent** of all identified network incidents, while password stealing attempts via HTTP account for **22.62 percent** of all household network incidents.

INDUSTRY. From a vertical perspective, infosecurity professionals estimated[5] that financial services (**43 percent**) and healthcare (**34 percent**) were among the most affected not just by the pandemic, but also by cybercriminals seeking to profit by seizing the moment and exploiting the fear, panic, and lack of information employees and organizations had regarding the Corona virus. With healthcare services and practitioners being instrumental in treating and keeping

3 "Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

4 "Mid-Year Threat Landscape Report 2020", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

5 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

Coronavirus patients stable, disruptions in their infrastructure would have placed patients' lives at risk. As such, Bitdefender has offered healthcare organizations of all sizes, from small dental and ophthalmic practices to large hospitals, free[6] access to our enterprise-grade security, at zero cost.

VULNERABILITIES. In terms of unpatched vulnerabilities in commonly installed applications and operating systems that threat actors seem to probe for in business environments, **36.37 percent of all reported unpatched vulnerabilities during the first half of 2020** involve CVEs that have been assigned in 2019, according to Bitdefender business telemetry. Of those, **88.39 percent** involve unpatched vulnerabilities in **Microsoft products and services**. However, while vulnerabilities in Microsoft products account for the bulk of exploitation attempts, threat actors may also seek to explore vulnerabilities in enterprise-grade device management software, popular network analysis tools used by IT and security professionals, text and source code editors, and even popular media player software.

OPPORTUNISTIC COVID-THEMED THREATS. Coronavirus-themed threats have also become the new norm, as Bitdefender telemetry found that attackers dress-up their threats with a cloak of panic, fear and information manipulation. Interestingly, coronavirus-themed threats and the actual coronavirus infections have evolved in a relatively similar way throughout March and April, potentially because as the virus spread across various countries in Europe threat actors prepared campaigns targeting those specific regions as well. Bitdefender telemetry has actually revealed that during this time span, **four in 10 emails on the Coronavirus topic are fraud, phishing, or malware.**

THE RISE OF APT AS A SERVICE. The new threat landscape that business and organizations were facing did not stop at opportunistic threat actors and the sudden change in workforce deployment. Recent Bitdefender investigations would find that advanced tactics and techniques usually attributed to state-sponsored APT groups were now part of attacks on verticals that were previously untouched by APT-style attacks. An APT-style cyberespionage attack targeting an international architectural and video production company revealed a new trend that small and mid-sized business have never included in their threat models: **APT hackers-for-hire**[7].

APTs-as-a-service mark a new trend in the evolution of cybercrime, as sophisticated attackers that were traditionally politically[8] or financially motivated, have now turned into mercenary APT groups offering their services to the highest bidder. MITRE's[9] matrix of advanced tactics and techniques is now something that any organization, regardless of size and field of interest, needs to consider for both increasing their chances of pinpointing sophisticated attacks, and evaluating security solutions that can offer the most complete and meaningful[10] coverage of the attack chain.

And it's not just companies that are affected by this new trend of APT-hackers-for-hire. Managed Service Providers (MSP) and have to face the reality that the tools and security services they offer clients need to offer the best of both worlds: security and visibility across any infrastructure.

The current cybersecurity skills shortage and lack of neurodiversity, coupled with this new trend, has created an opportunity for organizations that cannot build and staff their own IT and security teams with skills security professionals, to turn to managed detection and response services (MDR). These highly trained and skilled cybersecurity teams can bring forward the same security capabilities as an in-house Security Operations Center (SOC), but at a faction of the cost and wit no challenges in terms of skills shortage.

The threat landscape for businesses during the first half of 2020 has changed considerably in terms of attack surface, threats, and challenges brought forward by the global Coronavirus pandemic. Organizations that learn to adapt by understanding these new trends, will have the opportunity to both increase their cybersecurity resilience and strengthen their business continuity.

6 "Bitdefender Offers Enterprise-Grade Security at Zero-cost to Healthcare Organizations", Bitdefender, https://www.bitdefender.com/news/bitdefender-offers-enterprise-grade-security-at-zero-cost-to-healthcare-organizations-3815.html

7 "APT Hackers for Hire Used for Industrial Espionage", Bitdefender, https://labs.bitdefender.com/2020/08/apt-hackers-for-hire-used-for-industrial-espionage/

8 "StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure", Bitdefender, https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

9 MITRE, https://attack.mitre.org/

10 "MITRE ATT&CK Evaluation - Bitdefender a Stellar EDR Vendor For Midsized Organizations & MSPs", Bitdefender, https://businessinsights.bitdefender.com/mitre-attack-evaluation-results

MITRE ATTACK TACTICS AND TECHNIQUES. One of the biggest challenges for CIOs and CISOs is getting their message across to board members in a way that's unencumbered by tech jargon and at the same time eloquent and well-articulated enough that business decision makers understand the risks. More than **55 percent**[11] of CISOs and CIOs — many of whom have a seat at the most senior decision-making table in their organizations – believe that communication needs to change.

MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters to both classify attacks and assess an organization's risk, as well as identify and plug potential risks in their security infrastructure. MITRE's framework creates a common language shared by all infosec practitioners, making it easy to investigate and asses threats. Consequently, investigating and mapping out threats throughout their attack lifecycle shares the same taxonomy across all verticals and organizations. With remote employees changing the way business infrastructures have been architected, ATT&CK™ can both help spot, map, and understand threats, as well provide organizations with key and actionable information that can be used to strengthen their security posture.

The 'New Normal' Threats and Trends

During the first half of 2020, organizations have had to quickly adapt to a new way of managing their workforce as well as cope with new and unexpected threats and challenges. The Coronavirus pandemic has forced IT and security professionals to pull long shifts to accommodate full-time remote work capabilities for employees, while at the same time draft new security procedures and policies meant to limit the company's attack surface.

The pandemic has caused company infrastructures to be redesigned and support indefinite remote work, but the overnight changes made to policies and configurations are likely to have opened up new attack vectors that threat actors could exploit on the long run. If during 2019 the average time to detect and contain a data breach was estimated at around 209 days[12], it's likely that time will be significantly higher at the end of 2020, because of all the changes and misconfigurations infrastructures underwent as a result of the pandemic.

While some organizations fared better than others, it doesn't change the fact that **72 percent**[13] of CIOs and CISOs believe there is a need for a more diverse skill set in cybersecurity. The state of cyberwarfare as a threat to organizations has 71 percent of security professionals believing that it could be a threat to their organization, according to the same survey. While this belief is also shared by CIOs and CISOs, only 63 percent of them agree with the same statement.

It is this state of fear caused by being a potential collateral victim in a cyberwarfare incident that keeps security professionals up at night, and yet, **27 percent** of organizations have no strategy in place to protect against it.

Misconfiguration and risks

With the average time to contain a data breach estimated[14] at 206 days in 2019, it's likely that for 2020 that estimate will significantly increase because of misconfigurations that slipped by or because of a lack of visibility tools used to identify new potential blind spots caused by the new infrastructure reconfiguration.

11 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

12 "IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years", IBM, https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

13 "Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

14 "Cost of a Data Breach Report 2019", IBM, https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

In fact, one of the most reported misconfigurations found on business endpoints involves having the **WinRM[15] service enabled (87.31 percent)**, according to Bitdefender business telemetry. This remote management service allows IT and security teams to remotely manage endpoints and run various scripts on employee machines. This can be particularly useful when automating tasks and policies, but it can also be abused by threat actors if the service is misconfigured.

Coupled with the human risk component of having employees offsite and potentially connecting to company infrastructure through unsecure networks or even unmanaged systems added additional stress to security teams, tasked with redesigning security policies and infrastructure to cope with the new normal. Also, one of the biggest human risk when it comes to employees revolves around them **reusing old passwords (93.10 percent**), according to Bitdefender business telemetry.

Internet of Things

While the same survey points out that **75 percent** of CIOs and CISOs believe the more frequent use of IoT devices has increased their organization's security knowledge of how to protect them, 20 percent of CIOs and CISOs believe IoT devices will continue to spread faster than they can be secured.

This means that, while organizations have gained some experience throughout the past couple of years in terms of integrating IoTs and have even adapted their internal security policies to accommodate them, the constant proliferation of devices with little to no regard in terms of security standards or frameworks can still cause serious issues.

Enterprise Risks

Bitdefender's deceptive networks have been designed to observe these attack trends on IoTs by setting up and exposing vulnerable applications and services across the internet to learn how attackers behave and compromise these types of devices. Bitdefender's deceptive network either uses simulated protocols, such as Telnet or SSH, to interpret web exploits on various platforms, or use full-fledged and vulnerable Windows machines and exposes them online to threat actors to compromise them.

As a result, our deceptive networks register an average of **1.5 million hits every 15 minutes**, revealing that threat actors automate much of the scanning for vulnerable internet-connected devices. **Every 24 hours, more than 8.5 million web sessions are opened** by cybercriminals into our deceptive network. This reveals that many attacks revolve around manipulating session ID and cookies, all the way to performing directory traversal attacks on exposed web services.

Reporting almost **8,000 SSH sessions and 4,500 Telnet sessions every 24 hours**, Bitdefender's deceptive network technology collects around 200 files per hour that are usually dropped by hackers and threat actors. Besides malware, the files inlclude tools, scripts, and even exploits meant to either fully compromise the device or move laterally across the infrastructure.

All this telemetry serves to further strengthen the beliefs of CIOs and CISOs that proliferation of IoT is outpaces security standards and practices meant to protect them. Regardless of whether these IoTs are placed within home networks or corporate networks, many of their functionalities and used services and communication protocols are similar, meaning that most face the same risk regardless of the network they're connected to.

Remote Employees Risks

In terms of home users, while **61.56 percent of all traditional internet-connected devices** within households consist of smartphones, computers, tablets, laptops, consoles and routers, according to Bitdefender telemetry, IoTs make up the rest. Of non-traditional IoT devices, some of the most exotic examples of internet-connected devices include smart bulbs, smart vacuums, air purifiers, solar panels, baby monitors, cooking robots, motion sensors and many others.

Bitdefender telemetry has shown that the number of suspicious IoT incidents in households increased 46 percent from January to June. Port scanning attacks account for 55.73 percent of all identified network incidents, while password stealing attempts via HTTP account for 22.62 percent of all household network incidents.

15 "Windows Remote Management", Wikipedia, https://en.wikipedia.org/wiki/Windows_Remote_Management

Interestingly, recent surveys[16] reveal that home/commercial routers are have not been updated in more than a year, are riddled with hundreds of vulnerabilities and are running ancients OSs and EOL Linux kernels.

Bitdefender researchers have investigated[17] an instance in which a specific attack on home routers lead to threat actors altering DNS settings and redirecting victims to malware-serving websites. While this tactic was used at the time to convince victims to download and install Coronavirus-themed malware, it could also endanger remote employees as the same attack could potentially redirect them to a phishing website meant to collect corporate credentials and data. Consequently, successfully compromising home routers could potentially endanger not just remote employee data, but also companies.

Vulnerabilities

Patching remains one of the biggest challenges for organizations. Unpatched vulnerabilities are one of the main reasons for why organizations are breached, according to 60 percent[18] of breach victims in 2019, and the lack of visibility into these unpatched vulnerabilities usually leads to breaches. According to the same survey, 62 percent of organizations did not even know they were vulnerable until after the breach, and 52 percent have a manual patching procedure instead of an automated one.

Bitdefender's business telemetry revealed **63.63 percent of all reported unpatched vulnerabilities during the first half of 2020, involve CVEs that are older than 2018 (inclusively)**. This means that while **36.37 percent of all reported unpatched vulnerabilities during the first half of 2020, involve CVEs reported in 2019,** the vast majority of organizations still have unpatched vulnerabilities that were identified anywhere between 2002 and 2018.

Out of vulnerabilities reported in 2019, 88.39 percent involve unpatched vulnerabilities in Mozilla applications, and 7.91 percent in Microsoft products and services.

CVEs Distribution of Unpatched Vulnerabilities	
2019	36.37%
2018	31.27%
2017	19.37%
2016	4.76%
Other	8.23%

Most business environments a wide range of Microsoft and Mozilla versions are usually deployed, showing why attackers might focus on these particular vendors, but Bitdefender's business telemetry also spotted unpatched vulnerabilities for Oracle Virtual Box (1.77 percent), VLC Media Player (1.11 percent), and even Notepad++ (0.24 percent).

However, if these applications are fairly distributed across most companies, we've also found unpatched vulnerabilities for particular enterprise-grade software usually involved in asset management, identity management (IAM) platforms, and even popular archivers and network analysis tools commonly used by IT and security teams. From **HPE Intelligent Management Center (IMC), PuTTY, QUEMU and Squid to Atlassian, Extenua SilverSHielD, Wireshark, and MongoDB**, these are just a handful of popular business popular applications that have unpatched vulnerabilities, according to Bitdefender business telemetry. While the number of reported attempts at exploiting unpatched vulnerabilities in these enterprise-grade solutions is relatively small compared to Mozilla's or Microsoft's, it does reveal that attackers may also be interested in specifically compromising particular business software.

16 "Home Router Security Report 2020", Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

17 "New Router DNS Hijacking Attacks Abuse Bitbucket to Host Infostealer", Bitdefender, https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

18 "Costs and Consequences of Gaps in Vulnerability Response", Ponemon Institute & ServiceNow, https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

For example, during May 2020, the most reported unpatched 2019 high-severity vulnerability in a Mozilla product was CVE-2019-11746[19]. This particular vulnerability could be exploited in browser-like contexts and involves manipulating video elements that may cause an exploitable crash.

During the same timespan, the most reported unpatched 2019 high-severity vulnerability in a Microsoft product was CVE-2019-0541[20]. The vulnerability affects a wide range of Microsoft products ranging from Microsoft Office to Internet Explorer, and Office 365 ProPlus, and it could allow an attacker to take control of an affected system if the user is logged in with administrative user rights.

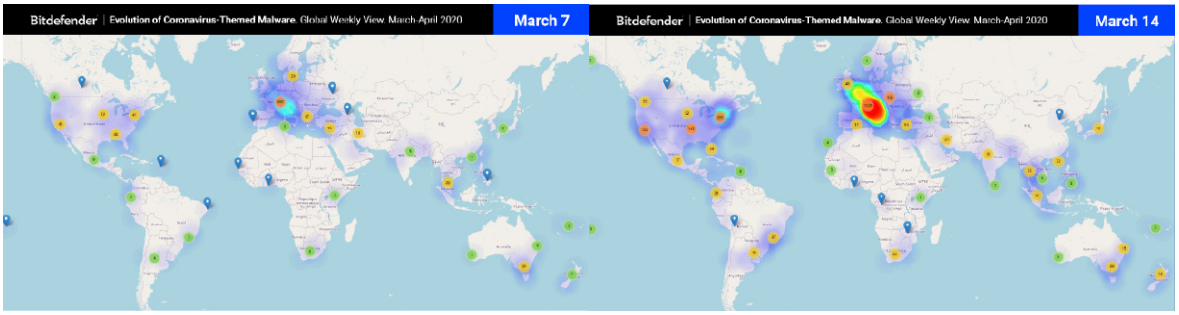
This telemetry from Bitdefender's patch management technology reveals that organizations still face challenges in actively and timely deploying patches and security updates for operating systems and applications. Either because of backward compatibility issues or because of failure to schedule and perform compatibility tests for their existing infrastructure, unpatched vulnerabilities can increase the risk of a data breach, especially in a work from-home-scenario where employee endpoints are no longer behind enterprise-grade hardware appliances meant to prevent exploits at the network layer.

With organizations having most of their workforce remote, setting and deploying patching policies has never been more crucial. With **six in 10 organizations** having machines with unpatched vulnerabilities that are older than 2018, the risks of having those vulnerabilities exploited by threat actors are higher than ever. A consistent and patching policy that's rolled out on all employee machines can significantly reduce the risk for organizations of suffering a data breach caused by an unpatched application.

Coronavirus-themed threats

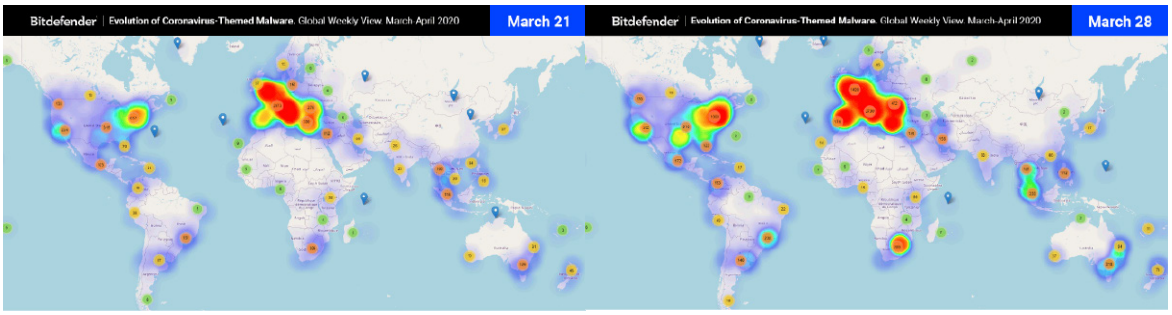
Themed Threats Overview

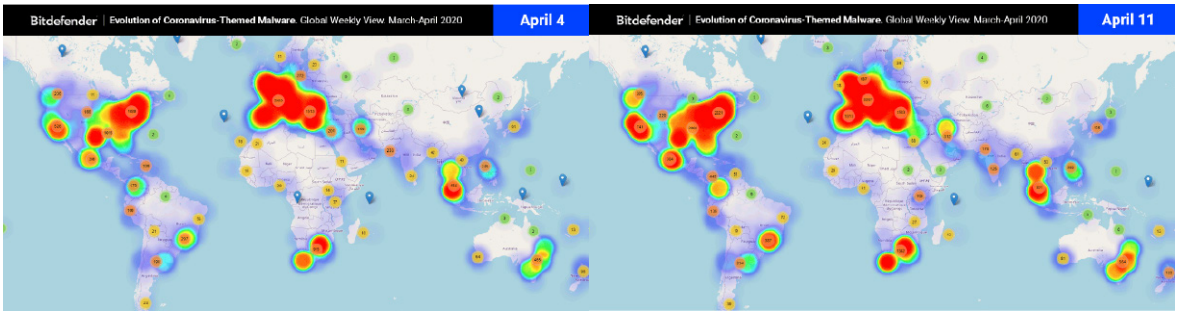
Over a timespan of seven weeks starting March 7, Bitdefender Coronavirus-themed telemetry reveals that threat actors have targeted countries in which the Coronavirus was also turning into a local pandemic. Countries like Spain, the United Kingdom, Italy and Germany seem to have been the hardest hit by both the biological threat as well as themed malware.

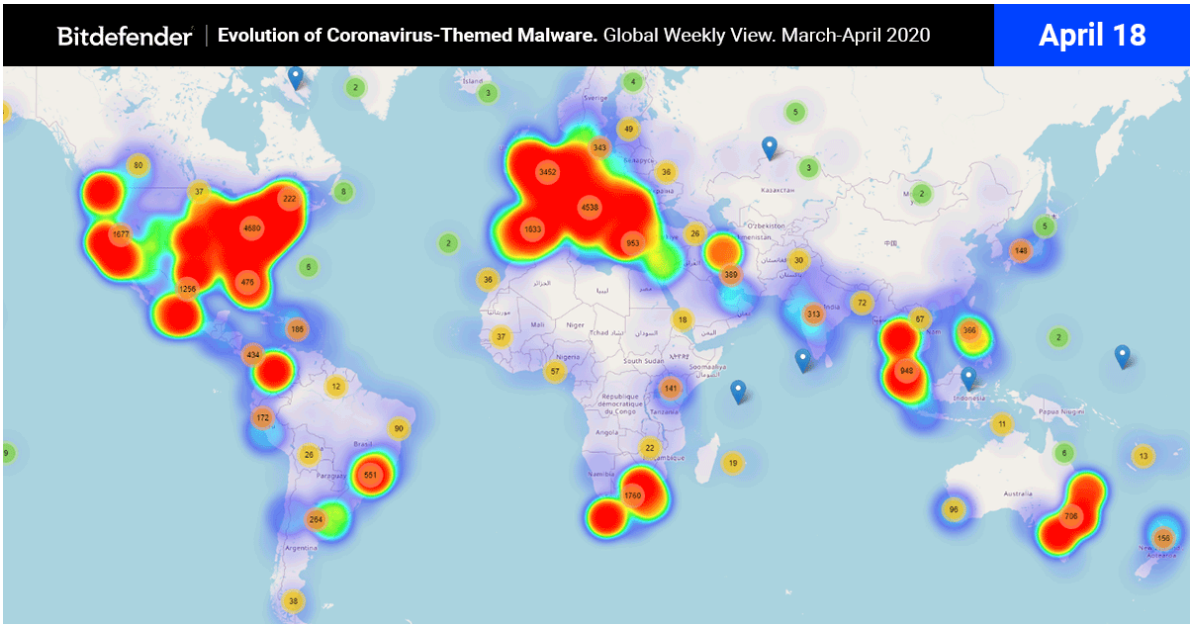


19 CVE-2019-11746, National Institute of Standards and Technology (NIST), https://nvd.nist.gov/vuln/detail/CVE-2019-11746

20 CVE-2019-0541, National Institute of Standards and Technology (NIST), https://nvd.nist.gov/vuln/detail/CVE-2019-0541







The coronavirus pandemic seems to have been a catalyst for threat actors amplifying their activity and quickly setting up opportunistic spam, fraud, and malware campaigns designed to trick victims into compromising their systems. What the heatmaps above reveal is that threat actors have constantly been up to date with local news and reports regarding the evolution of the pandemic in specific countries, fine-tuning their messages to exploit the fear and panic caused by the outbreak.

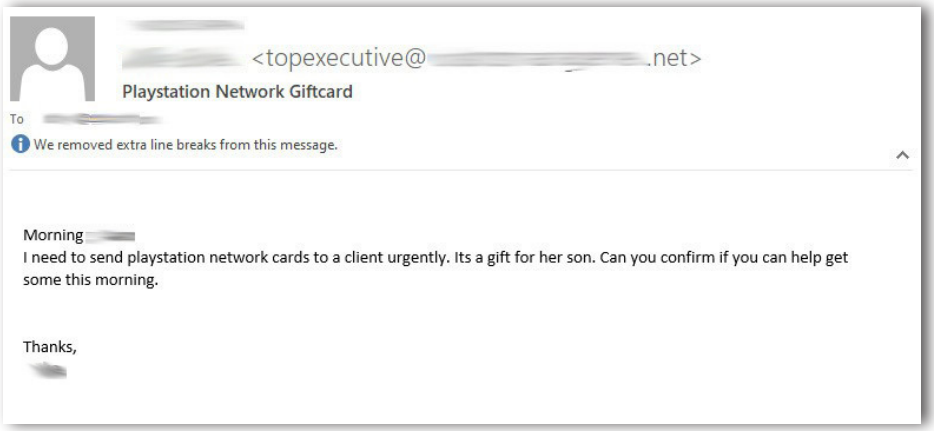
Traditionally, most spam, phishing and fraudulent emails were designed to have simply-constructed messages, whose primary purpose was to trick the victim into opening a tainted attachment or a link. However, all that changed as messages were carefully constructed and worded so that they seem believable, legitimate, and of high importance. Focusing more on the social engineering part and building credibility, coronavirus-themed threats and messages targeted companies across all verticals, preying on the general lack of information caused by the pandemic.

Phishing and Spearphishing

Perhaps one of the biggest challenges for employees in terms of remote work is falling prey to phishing and spearphishing emails. Before the pandemic, any suspicious email received from a would-be colleague would have easily been dismissed by waking up to their desk and asking for confirmation. Remote work has removed the physical conformation aspect of seemingly legitimate work emails, potentially exposing businesses to more business email compromise (BEC) attempts than ever.

The pandemic has proven to be a strong catalyst for opportunistic coronavirus-themed spam emails which spiked considerably throughout the first half of 2020. Bitdefender telemetry shows[21] that **four in 10 coronavirus-themed emails have been classified as spam, phishing, or malware**, suggesting that remote employees and average users have been constantly at risk of opening up tainted emails. While endpoint and employee data security was potentially at risk, so were corporate infrastructures that could have been affected by threats embedded within these emails or URLs that could have escalated and raised the organization's risk factor.

Cybercriminals are nothing if not opportunistic and BEC emails have started using the same jargon and approach that office colleagues have started using since the pandemic hit. Most BEC emails seem to be short, personal and they are always phrased as if the victim needs to perform a quick action or a favor for a coworker.



21 "Mid-Year Threat Landscape Report 2020", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

Others are more generic in nature and tend to emulate the same style used by internal IT team or by automated internal platforms. The end goal is to trick the employee into either replying to the email and engaging into a real-time conversation with the threat actors or simply compromise the endpoint by either downloading malware or giving away authentication credentials on attacker-controlled websites.

Business email compromise has evolved[22] over the past couple of years in terms of approached themes, ranging from wage and tax statements in 2016 to human resources and gift cards in 2018. If during 2019 the main BEC topics revolved around healthcare and payroll diversion, 2020 seems to have been all about COVID-19 and healthcare, according to HHS.

BEC scams play a niche role in the overall phishing scheme, but are estimated to be the most damaging, with losses estimated at nearly $75,000[23], per complaint in 2019, on average, and a total of $1.7 billion, according to the FBI. As the pandemic was a global phenomenon in 2020, it is likely that BEC financial losses will far exceed those of 2019.

Beyond WFH. Significant shifts in advanced attacks.

Adversarial Tactics and Techniques

Communication is key when discussing cyber risk and **55 percent[24] of CIOs and CISOs believe that this needs to change** dramatically if they want to increase investment. The Massachusetts Institute of Technology Research (MITRE) Attack Tactics and Techniques framework has become the security standard to which all organizations map their security incidents. Because it provides a comprehensive list of tactics and techniques threat actors have commonly used throughout their attacks, it can help map out security incidents from the initial point of compromise, all the way to lateral movement, persistence, and data exfiltration.

Security incident reports mapped onto this framework have become the new norm because it allows security professionals to use the same language when describing a security incident. However, most of the capabilities needed to map out all these tactics are usually bundled within Endpoint Detection and Response (EDR) solution from security vendors, giving forensic and security teams to have a complete picture of the events leading up to a breach, and after.

Meaningful coverage of the attack chain is the ultimate goal for organizations as it can help them understand what their blind spots are and how they can be addressed, and also strengthen their security posture by having visibility across the entire attack chain, blocking attacks before they reach their final goal. Organizations are all about minimizing risks and the MITRE framework can help with that.

Malicious Scenarios – A WMI Case Study

It's not uncommon for threat actors to (ab)use tools and applications that are part of the operating system to perform malicious actions. For example, some of the most-used tools that are often abused by threat actors involve the use of PowerShell or even WMI (Windows Management Instrumentation).

If we are to only analyze how threat actors and malware abuses WMI, we'll notice that MITRE ATT&CK® framework covers a lot of scenarios in which WMI can be abused throughout each step of the attack lifecycle, ranging from

22 "Business Email Compromise in the Health Sector", U.S. Department of Health and Human Services (HHS), https://www.hhs.gov/sites/default/files/business-email-compromise-in-the-health-sector.pdf

23 "2019 Internet Crime Report", Federal Bureau of Investigation (FBI), https://pdf.ic3.gov/2019_IC3Report.pdf

24 "Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

execution and persistence to defense evasion, discovery, lateral movement, command and control, and even exfiltration.

For example, one of the most notorious examples in which WMI played a massive role involves the 2010 **Stuxnet**, which affected nuclear processing facilities in Natanz, Iran and used WMI to enumerate users and spread to available network shares.

Mapping **Stuxnet's use of WMI according to MITRE's framework**, we have the following:

Persistence:
- Technique T1084 - Windows Management Instrumentation Event Subscription

Discovery:
- Technique T1087 - Account Discovery
- Technique T1135 - Network Share Discovery

Lateral Movement
- Technique T1105 - Remote File Copy

Since then, most malware and threats regardless of their sophistication have been leveraging the power of WMI throughout various steps in the attack chain.

For instance, the **Kingminer crypto-jacking malware abuses WMI** Event Subscription mechanism in the Execution stage: one part of the malicious script registers an active script consumer to execute periodically. The WMI event consumer ensures persistence by using the **T1546.003, Event Triggered Execution: Windows Management Instrumentation Event Subscription**.

The **Maze ransomware**[25] has become one of the most popular ransomware families, filling in the void left behind by the now-defunct GandCrab ransomware family. Maze authors implemented an exfiltration mechanism to leverage payment and transform an operational issue into a data breach. Using the WMI, Maze destroys any existing Windows backups, such as the Volume Shadow Copies. By **querying the Win32_ShadowCopy WMI class**, it finds the shadows to be deleted in the next phase, also known as **Technique T1490, Inhibit System Recovery**.

Emotet, also known as Geodo or Mealybug, was first detected in 2014 and has remained active ever since. The most common entry vector for Emotet is spearphishing email attachments, also known as Technique T1566.001, Phishing: Spearphishing Attachment. However, in terms of tactics and techniques, recent versions often **use Windows Management Instrumentation to remain undetected**. To achieve this, it mainly uses **Technique T1202, Indirect Command Execution**, with the Win32_Process WMI class, instead of simply spawning PowerShell directly, allowing it to sometimes fly under the radar.

By understanding how WMI works and how it can be (ab)used by attackers and malware, companies can set up and deploy WMI usage policies that reduce risk of misuses.

While there are other examples of malware abusing WMI throughout their attack lifecycles, the MITRE's framework provides the common language and taxonomy used to describe every phase of the attack and map it to a tactic or technique. While malware, attackers, and threats in general have significantly increased in sophistication throughout the last decade, the MITRE framework can be the perfect tool for both analyzing and understanding how threats operate, and help organizations use this knowledge to augment their security posture.

25 "A Malware Researcher's Guide to Reversing Maze Ransomware", Bitdefender, https://labs.bitdefender.com/2020/03/a-malware-researchers-guide-to-reversing-maze/

2020 Popular MITRE ATT&CK® Techniques and Sub-Techniques

Bitdefender's business telemetry on identifying the most commonly used attack tactics and techniques used by sophisticated hackers has revealed that phishing remains one of the most common tactics reported for initial access.

One of most commonly used tactic during the **Execution** stage is referred to as **"Command and Scripting Interpreter" (T1059)** by the MITRE ATT&CK® Matrix for Enterprise and it accounts for 21.37 percent of all the tactics reported by Bitdefender's telemetry. One of the most popular sub-techniques (T1059.001) for this tactic revolves around the use of PowerShell commands and scripts and accounts for **42.52 percent of the total number of reported T1059 sub-techniques**. This is a popular tactic employed by adversaries as PowerShell can be used to automate tasks and it's already present on the victim's machine. Also, PowerShell commands and scrips can be executed without specifically invoking the "powershell.exe" binary, but by using interfaces to it's underlying components exposed via Windows Common Language Interface (CLI).

In terms of **Persistence** tactics, one of the most reported technique used is the **T1546 - Event Triggered Execution**, which is responsible for mapping out various systems events that could be indicative of threat actors trying to tamper with system registries or actions that could allow them to gain persistence on the machine. For example, the most encountered sub-technique reported by Bitdefender business telemetry in terms of Event Triggered Execution is the T1546.001 - Change Default File Association, which accounts for **31.54 percent of all reported sub-techniques for T1546**. This is particularly useful for threat actors as it allows them to change registry related to file associations, and then execute commands set up as subkeys for those shell keys. Changing default program associations can enable attackers to trick the OS into executing commands or opening tainted documents.

Privilege Escalation techniques are also part of the attack chain that threat actors use for gaining higher-level permissions on a victim's machine or infrastructure and one of the post reported technique is T1134 - Access Token Manipulation. However, one of the most commonly reported sub-technique involve **T1134.002 - Create Process with Token**. Threat actors duplicate an access token, usually for a user with administrative privileges, and use it to create a new process that runs under the security context of an impersonated user. This attack technique can be easily mitigated by limiting permissions to users and user groups so they cannot create access tokens, as well as auditing command-line activity for commands that involve privilege elevation.

Part of **Defense Evasion** techniques, Bitdefender's business telemetry found that the T1562 - Impair Defenses technique seems to be the most used tactic. In terms of sub-techniques, the **T1562.006 - Indicator Blocking** seems to be of particular interest to threat actors, it involves disabling various security sensors responsible for collecting and analyzing data.

The **Credential Access** technique is also quite popular as threat actors often try to obtain credentials that are insecurely stored. However, one of the most reported sub-techniques involves **T1552.002 - Credentials in Registry, which accounts for 20.27 percent of all reported sub-techniques for T1552 - Unsecured Credentials**. This points to threat actors searching registry keys using credential dupers or specifically querying registry keys belonging to popular SSH and telnet clients, in order to find insecurely stored credentials that they can use. Both APT groups have been known to employ this mechanism, as well as various Trojans, such as the TrickBot Trojan.

The **Discovery** part of the attack chain is also vital during reconnaissance, as it allows threat actors to identify potential high-value targets such as administrator accounts. One of the reported Discover techniques by Bitdefender business telemetry involves the T1087 - Account Discovery technique. However, the most reported sub-technique, with **66.58 percent of the total reported Account Discovery sub-techniques**, involves **T1087.002 - Domain Account**. This reveals that threat actors are mostly interested in listing user accounts within a domain, potentially to find those with administrative rights. A simple mitigation to this technique involves setting a policy that prevents administrator accounts from being enumerated.

Lateral Movement techniques are another thing to worry about, as attackers often try to probe the compromised network for other valuable targets by using SSH or VNC services. However, in terms of sub-techniques, the **T1021.002 - SMB/Windows Admin Shares** seems to be the most reported of the **T1021 - Remote Services** techniques, suggesting

threat actors might be trying to interact with remote network share using Server Message Block (SMB). These SMB shares can sometimes be very useful for sophisticated threat actors as they can be used for file storage and exfiltration.

In terms of **Command and Control** techniques, the T1071 - Application Layer Protocol seems to have been the most reported by Bitdefender business telemetry, with two particular sub-techniques, **T1071.002 - File Transfer Protocols** and **T1071.003 - Mail Protocols**, being the most popular. This means that threat actors constantly communicate with command and control infrastructures either via file transfer protocols such as FTP, FTPS, and TFPT or via email protocols such as SMTP/S, POP3/S, and IMAP. These are very common communication protocols within organizations and usually fly below the radar of security solutions designed to flag suspicious communication protocols.

In terms of Impact, the final stage of the attack chain, one of the most reported technique involves T1565 - Data Manipulation. However, the **T1565.003 - Runtime Data Manipulation sub-technique accounts for 72.91 percent** of all reported sub-techniques for Data Manipulation. This means that threat actors often try to manipulate data to cause runtime manipulations or modify the output of a specific application.

Rise of APTs as a service

Throughout the first half of 2020, Bitdefender researchers investigated a series of APTs and attacks that have revealed new insights into how APT groups have evolved. Traditionally, APT groups have been either state-sponsored or strictly financially driven, with operations usually targeting government entities based on some political agenda, or going after financial institutions.

An investigation in early 2020 revealed an attack by an Iranian APT group, known as Chafer[26], targeting air transportation in and government institutions in Kuwait and Saudi Arabia. Some of the attack tactics and techniques employed by the group are not uncommon to APTs, ranging from using spearphishing as an initial attack vector, to creating their own user accounts for persistency, and even lateral movement through sometimes custom-made tools. A particularly interesting aspect of the Chafer APT group is that both attacks were likely focused on data exfiltration and attacker activity occurred during weekends.

A later investigation into another APT group, dubbed BitterAPT[27], also found evidence that the group has some political affiliations. Based on targeted regions and victims' profiles revealed by security researchers in the past, BitterAPT has been known to target victims in Pakistan, China, India, and other countries in South Asia, as well as Saudi Arabia. Bitdefender's investigation revealed previously unknown Android applications that seem to have targeted religious groups by masquerading as True Islam or Saima Eid related applications as well as variations that are more generic, imitating common applications such as Voice Mail, chat, image viewers and WhatsApp activators.

Interestingly, forensic evidence left behind by timestamps (Monday to Friday between 9 AM – 5 PM) on analyzed samples seem to indicate that the group is also state sponsored. The same timestamps seem to indicate that the group is based in a South Asian country.

Digging deeper into their previous operations, both 2014 and 2019 campaigns seem to have used applications posing as local news aggregators for Kashmir. Considering that both 2014 and 2019 were election years in that region, there's a good chance that the BitterAPT could be state-sponsored.

Perhaps one of the most interesting developments in the behavior of APT groups occurred when Bitdefender researchers investigated an APT group, named StrongPity[28], targeting victims in Turkey and Syria using watering hole tactics to selectively infect victims. While the group has been known to target victims in Belgium and Italy, this

26 "Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia", Bitdefender, https://labs.bitdefender.com/2020/05/iranian-chafer-apt-targeted-air-transportation-and-government-in-kuwait-and-saudi-arabia

27 "BitterAPT Revisited: the Untold Evolution of an Android Espionage Tool", Bitdefender, https://labs.bitdefender.com/2020/06/bitterapt-revisited-the-untold-evolution-of-an-android-espionage-tool/

28 "StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure", Bitdefender, https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

particular attack focused on the Kurdish community in Turkey and Syria seems to have coincided with a Turkish military operation. October 1st 2019 was the date for both when the military operation started and the timestamp on the StrongPity APT samples.

The advanced tactics, tools, and infrastructure used by the StrongPity APT group suggests that it is both capable and potentially state sponsored. However, the group has been flying below the radar since 2016, when it was first reported.

In one of the most recent investigation conducted by Bitdefender researchers, we managed to gain a first-hand glimpse into how APT groups have evolved. Just as traditional malware has evolved into an as-a-service business model, with ransomware soon to follow on the same trend, APT groups seem to have made the same change.

A cyberespionage attack targeting an international architectural and video production company has revealed that APT groups may no longer be motivated by political agenda, but instead could be offering their services to the highest bidder. One of the major findings of the investigations was that the initial attack vector when targeting the architectural company was a zero-day vulnerability in a popular 3D computer graphics software (Autodesk 3ds Max) that the company was using.

The architectural company is known to have been collaborating in billion-dollar real estate projects in New York, London, Australia, and Oman. Based on tactics and techniques employed by the APT group to compromise the target, it's likely the group is a potential APT mercenary group used for industrial cyberespionage.

Industrial espionage is nothing new, and, since the real estate industry is highly competitive, with contracts valued in the billions of dollars, the stakes are high for winning contracts for luxury projects. In the minds of some, this could justify turning to mercenary APT groups for gaining a negotiation advantage.

Network-based Threats

Business infrastructures are both about applications and networks. If unpatched vulnerabilities in applications and operating systems can expose machines to a wide range of malware and cybercriminals, network-based threats could allow threat actors to both probe and map your infrastructure and compromise high-value data.

For instance, during the past couple of years, ransomware operators have shifted their attacks from a shotgun shell approach, in which they compromised victims via traditional attack vectors like spearphishing, to a more targeted approach. Abusing remote desktop protocol, exploiting unpatched vulnerabilities in the SMB protocol and even bruteforcing credentials for FTP or RDP sessions have been the most common attack tactics for compromising business environments.

Bitdefender's network attack defense technology has found that **46.84 percent of all network-level attacks involve exploiting a vulnerability in the SMB protocol**. Out of these, the **DoublePulsar[29] backdoor implant accounts for 90.74 percent of used SMB exploits**. While this might suggest that some organizations may still be vulnerable to the exploit, it is also likely that DoubelPulsar has become the go-to tool for cybercriminals looking to move laterally across infrastructures when probing for network vulnerabilities.

Network-based Attacks Distribution	
SMB Exploits	46.84%
Bruteforce Attacks (FTP, RDP)	41.63%
Other	11.53%

SMB vulnerabilies such as EternalBlue[30], EternalDarkness, EternalChampion and even EternalRomance are amongst the top SMB exploits being used to compromise business networks. However, it's likely they're all bundled in various

29 DoublePulsar, Wikipedia, https://en.wikipedia.org/wiki/DoublePulsar

30 EternalBlue, Wikipedia, https://en.wikipedia.org/wiki/EternalBlue

network exploiting tools and used in cascade until one manages to compromise an unpatched system.

The same telemetry also revealed that **bruteforce attacks on RDP and FTP services account for 41.63 percent of all network-level attacks in business infrastructures**. Successfully gaining access to these services means threat actors could take remote control of enterprise machines and endpoints, or even access internal FTP shares where sensitive data is usually stored. However, if we look at the current threat landscape for businesses, many attacks on these services involve ransomware operators seeking to gain a foothold within the organization, seek out valuable data, and then manually deploying ransomware with a custom payload and high ransom note.

Consequences - SMBs Now Facing a New Threat

APT mercenaries could change the way small and mid-sized business build their threat models. One of the biggest recent fears for IT and security decision makers is that their company could be targeted by APT groups. If in the past, most APT-level breaches of SMBs were part of supply chain attacks, APT mercenaries offering their services to the highest bidder could practically mean open season for small and medium-sized companies.

Traditionally, small and medium-sized businesses only relied on threat models that dealt with the current threat landscape or maybe risks associated with employees, APT mercenaries completely change the premise for security for these companies. Threat models that factored in state-sponsored actors and advanced actors were mostly on the agenda for large companies and government-based infrastructure. The commoditization of APT hackers-for-hire means that any company, regardless of its size or vertical, could be facing state-sponsored sophisticated attacks bent on industrial espionage.

Small and medium-sized companies should be focusing on augmenting their security stack with more than just malware-detecting security software, but with visibility tools both at the endpoint and network layers. For example, automated endpoint detection and response tools that focus relevant security warnings indicative of a tactic or technique commonly used by APT groups could easily flag potential intruder. Also, the lack of qualified security personnel could be addressed by turning to managed detection and response teams that both asses the company's infrastructure and propose security and hardening tools, and act as specialized security hunting team that perform threat hunting on suspicious events. Both EDR and MDR have become accessible to small and medium-sized companies, offering SOC-like security that only large organizations could usually afford, but at a fraction of the cost.

Regional Evolution of Traditional Threats

While the business threat landscape is constantly evolving with organizations regularly investing in security technologies and building new strategies for detection and risk mitigation, threat gunning for their infrastructure never sleep.

Bitdefender business telemetry related to traditional threats, such as ransomware, coin miners, fileless malware, and even Potentially Unwanted Applications (PUA), has revealed that they still pose a threat to organizations.

Although the ransomware market is fragmented into a wide range of families each offered as-a-service by ransomware operators, the number of complains[31] registered by the FBI in 2019 has reached 2047 and an estimated $8.9 million in losses. However, this only accounts for companies that have actually reported a ransomware incident to authorities in the United States. In reality, ransomware has been a lucrative business for a long time and has been generating billions in paid ransom notes for cybercriminals.

31 "2019 Internet Crime Report", Federal Bureau of Investigation (FBI), https://pdf.ic3.gov/2019_IC3Report.pdf

One of the newest developments for ransomware is the addition of an extortion component. After compromising an organization, ransomware operators will often find and exfiltrate sensitive company data before deploying ransomware. That way, if the company refuses to give in to ransom demands, ransomware operators can threaten to publish the stolen data, forcing the company to be liable for a GDPR fine potentially greater than the requested ransom note. While it's never advisable to give in to ransomware demands, but treat the incident as a hardware failure, giving in only serves to further encourage and sponsor ransomware operators. Looking at the global evolution of ransomware reports from our business telemetry, it's safe to say that this particular threat is not going anywhere. There have sufficient incidents reported in the media with outages caused by potential ransomware incidents, affecting everything from hospitals to government. While the number of global ransomware reports might seem to go down starting April 2020, it's likely that work-from-home situation created new opportunities for cybercriminals in terms of extortion and potential data exfiltration.

H1 2020	Ransomware
Jan	19.50%
Feb	19.33%
Mar	17.85%
Apr	14.02%
May	15.01%
Jun	14.29%

Global coin miner reports generated by our business telemetry also indicate that coin miners are still something that cybercriminals are looking into. Either by leveraging an organizations' cloud computing power after successfully compromising their systems or by tainting various applications to run coin mining software, the threat is still present for business environments. Although most coin miner reports occurred during the first three months of 2020, the last three months still account for 38.91 percent of all detection during the first half of 2020.

H1 2020	Coin Miner
Jan	20.63%
Feb	21.77%
Mar	19.10%
Apr	12.94%
May	12.94%
Jun	13.03%

Global fileless malware reports from our business telemetry have also revealed that threat actors still leverage living-off-the-land tools for compromising business environments. Either by tricking employees into running tainted attachments or by using exploiting unpatched vulnerabilities to run fileless malware, businesses still need technologies and policies designed to detect and block these threats.

H1 2020	Fileless
Jan	25.25%
Feb	24.26%
Mar	16.83%
Apr	10.89%
May	8.42%
Jun	14.36%

Potentially Unwanted Applications in business environments can occur if employee security policies are sometimes to relaxed, allowing users to install and use software that's not sanctioned by IT and security teams. While PUAs are not malicious in the way malware is, they can install additional components, it may allow threat actors to plant backdoors, or they may simply be a nuisance by displaying ads and popups and making the overall user experience really cumbersome. Interestingly, our business telemetry indicates that PUA reports during the first half 2020 only peaked in March (18.22 percent of the total number of PUA reports during the first half of 2020), maintaining a relative constant presence throughout the year.

H1 2020	PUA
Jan	15.72%
Feb	16.74%
Mar	18.22%
Apr	15.74%
May	16.87%
Jun	16.72%

United States

H1 2020	Ransomware
Jan	20.34%
Feb	16.96%
Mar	17.26%
Apr	15.19%
May	16.36%
Jun	13.89%

H1 2020	Coin Miner
Jan	15.98%
Feb	17.96%
Mar	20.13%
Apr	15.81%
May	15.81%
Jun	14.31%

H1 2020	Fileless
Jan	33.33%
Feb	11.11%
Mar	11.11%
Apr	33.33%
May	0.00%
Jun	11.11%

H1 2020	PUA
Jan	15.69%
Feb	15.84%
Mar	17.17%
Apr	16.41%
May	17.78%
Jun	17.11%

United Kingdom

H1 2020	Ransomware
Jan	16.64%
Feb	17.96%
Mar	18.26%
Apr	18.50%
May	14.23%
Jun	14.41%

H1 2020	Coin Miner
Jan	18.18%
Feb	24.56%
Mar	18.32%
Apr	13.36%
May	13.36%
Jun	12.08%

H1 2020	PUA
Jan	15.58%
Feb	16.10%
Mar	17.85%
Apr	16.38%
May	17.07%
Jun	17.01%

Sweden

H1 2020	Ransomware
Jan	20.55%
Feb	17.81%
Mar	23.29%
Apr	20.55%
May	9.59%
Jun	8.22%

H1 2020	Coin Miner
Jan	18.75%
Feb	25.00%
Mar	21.05%
Apr	12.50%
May	12.50%
Jun	8.55%

H1 2020	PUA
Jan	15.27%
Feb	15.63%
Mar	16.72%
Apr	18.54%
May	17.85%
Jun	15.99%

Romania

H1 2020	Ransomware
Jan	14.66%
Feb	13.91%
Mar	11.52%
Apr	12.12%
May	24.23%
Jun	23.56%

H1 2020	Coin Miner
Jan	22.88%
Feb	22.39%
Mar	18.65%
Apr	14.09%
May	14.09%
Jun	10.71%

H1 2020	PUA
Jan	13.07%
Feb	14.17%
Mar	18.44%
Apr	16.05%
May	19.15%
Jun	19.12%

Italy

H1 2020	Ransomware
Jan	19.01%
Feb	17.27%
Mar	17.55%
Apr	15.32%
May	15.81%
Jun	15.04%

H1 2020	Coin Miner
Jan	16.41%
Feb	26.79%
Mar	16.67%
Apr	13.08%
May	13.46%
Jun	13.59%

H1 2020	PUA
Jan	16.14%
Feb	15.80%
Mar	17.91%
Apr	15.79%
May	17.80%
Jun	16.55%

France

H1 2020	Ransomware
Jan	19.48%
Feb	19.85%
Mar	19.73%
Apr	12.45%
May	14.55%
Jun	13.93%

H1 2020	Coin Miner
Jan	21.15%
Feb	22.94%
Mar	21.23%
Apr	15.11%
May	10.98%
Jun	8.60%

H1 2020	PUA
Jan	15.38%
Feb	15.78%
Mar	18.73%
Apr	16.31%
May	17.16%
Jun	16.63%

Spain

H1 2020	Ransomware
Jan	20.56%
Feb	16.70%
Mar	14.59%
Apr	13.36%
May	18.80%
Jun	15.99%

H1 2020	Coin Miner
Jan	16.80%
Feb	28.74%
Mar	17.99%
Apr	11.78%
May	11.39%
Jun	13.30%

H1 2020	PUA
Jan	17.77%
Feb	17.80%
Mar	18.13%
Apr	14.71%
May	15.57%
Jun	16.03%

Denmark

H1 2020	Ransomware
Jan	23.66%
Feb	14.52%
Mar	19.35%
Apr	16.67%
May	15.05%
Jun	10.75%

H1 2020	Coin Miner
Jan	15.53%
Feb	26.89%
Mar	17.05%
Apr	12.88%
May	14.77%
Jun	12.88%

H1 2020	PUA
Jan	16.04%
Feb	15.00%
Mar	17.06%
Apr	16.42%
May	18.11%
Jun	17.38%

Germany

H1 2020	Ransomware
Jan	23.01%
Feb	18.25%
Mar	21.12%
Apr	14.20%
May	12.97%
Jun	10.46%

H1 2020	Coin Miner
Jan	21.07%
Feb	20.05%
Mar	19.04%
Apr	15.48%
May	12.06%
Jun	12.31%

H1 2020	PUA
Jan	14.89%
Feb	15.57%
Mar	18.58%
Apr	17.01%
May	17.50%
Jun	16.46%

Australia

H1 2020	Ransomware
Jan	9.51%
Feb	14.17%
Mar	18.41%
Apr	15.90%
May	22.47%
Jun	19.53%

H1 2020	Coin Miner
Jan	13.96%
Feb	23.72%
Mar	18.39%
Apr	15.32%
May	14.64%
Jun	13.96%

H1 2020	PUA
Jan	11.31%
Feb	15.25%
Mar	19.22%
Apr	18.51%
May	18.35%
Jun	17.36%

Netherlands

H1 2020	Ransomware
Jan	17.52%
Feb	17.08%
Mar	16.35%
Apr	17.37%
May	14.60%
Jun	17.08%

H1 2020	Coin Miner
Jan	19.71%
Feb	23.22%
Mar	17.44%
Apr	13.93%
May	13.48%
Jun	12.23%

H1 2020	PUA
Jan	14.59%
Feb	15.45%
Mar	18.87%
Apr	17.55%
May	17.82%
Jun	15.73%

Conclusions

The business threat landscape has evolved to the point where all organizations, regardless of size or vertical, seem to face the same threats. The recent global pandemic has acted as a catalyst for a new wave of BEC themed of attacks, obliging companies to update their training and awareness programs.

The new normal for businesses now includes employees working remotely, meaning that threat actors have expanded their attack surface to include internet-facing infrastructures and services that were previously shielded, as well as company endpoints that are now away from the corporate network. Vulnerabilities, misconfigurations, and the overall cybersecurity skills shortage have companies facing new challenges and risk that most did not even conceive of 12 months ago.

APT hackers-for-hire have changed the way small and medium-sized businesses need to approach security and integrate this new threat into their threat models. Failure to do so as well as failure to properly secure their infrastructure could inflict loss of business, or worse. Managed Detection and Response services and endpoint detection and response technologies can compensate for these new challenges and help organizations face these new threats, without taxing their security budgets.

Since the first half of 2020 was marked by a rapid change in infrastructure deployments, personnel shifts, and new threats, most businesses have faced one of their biggest challenges to date.

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security
NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test
SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row
More MSP-integrated solutions than any other security vendor
3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**
Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Whitepaper-ThreatReport2020-creat-4889-en_EN
11/05/20November 6, 2020 12:52 pm11/06/20