

Global Incident Response Threat Report

COVID-19 Continues to Create a Larger Surface Area for Cyberattacks

Incident response professionals note an increase in counter IR and island hopping

Tom Kellermann, Head of Cybersecurity Strategy

Rick McElroy, Security Strategist

August 2020



Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

Executive summary

It may feel a long way off now, but on February 29, 2020, officials in the Seattle area announced the first U.S. COVID-19 fatality. That, however, wasn't the only bad news. The fear and paranoia coursing through the world left organizations particularly vulnerable to cyberattacks – which shot up by an estimated 66%.

It's not difficult to see why this might be the case. Imagine it: An email comes through offering new workplace safety protocols, and an employee, worn down by the events of the day or feeling anxious about their safety, clicks through. The attacker enters the network. Factor in a sea of newly remote workers and overloaded security teams, and it's easy to see how COVID-19, as Tom Kellermann, head of cybersecurity strategy at VMware Carbon Black, notes, "becomes a panacea for cybercriminals."

"Not only has the corporate perimeter been broken," he explains. "But people are hungry for new online experiences, and using new, smart technologies to find them. And hackers know it."

COVID-19 has exacerbated preexisting cyberthreats, from counter incident response and island hopping to lateral movement and destructive attacks. These attacks are ratcheting up existing geopolitical tensions.

Rick McElroy, cybersecurity strategist at VMware Carbon Black, frames it this way: "If I'm a cybercriminal, the pool of people I can trick now is exponentially larger, simply because it's a global disaster."

Organizations, most of which depend on VPNs and other traditional network security infrastructure, may not be prepared. Stopping today's increasingly sophisticated cyberattacks, whether they're COVID-19-related or not, will mean adopting next generation IR strategies.

We hope that in this, the fifth installment of VMware Carbon Black's semiannual Global Incident Response Threat Report, you'll find a clearer picture of the evolving threat landscape as well as actionable guidance for today, tomorrow and the challenging months to come.

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

Key highlights

53%

With COVID-19 comes a surge in cyberattacks. Security teams are struggling to keep up.

53% of IR professionals we surveyed encountered or observed an increase in cyberattacks exploiting COVID-19. They pointed to remote access inefficiencies (52%), VPN vulnerabilities (45%) and staff shortages (36%) as the most daunting endpoint security challenges in this regard.

33%

Counter IR explodes as adversaries fight for persistent attacks on systems.

A third of respondents (33%) encountered instances of attempted counter IR in the 90 days before they took our survey – a 10% increase from our previous report. The forms of counter IR used – mostly destruction of logs (50%) and diversion (44%) – signal attackers' increasingly punitive nature and the rise of destructive attacks more broadly.

51%

The financial industry is under siege.

More than half of attacks (51%) in the 90 days prior to this survey have been on the financial sector, followed by healthcare (35%), professional services (35%) and retail (31%). This correlates with the finding that 59% of those surveyed said attackers' end goal was financial gain – by far the leading motivation.

33%

One in three attacks shows signs of lateral movement

– and as common tools like PowerShell bolster their defenses, this movement is being facilitated increasingly by the misuse of WMI, Google Drive and process hollowing.

51%

Cyberthreats from China are increasing.

Over half of respondents (51%) saw attacks from China in the 90 days before this survey was held, followed by North America (40%) and Russia (38%). As Kellermann notes, “The Chinese have exhibited a dramatic evolution in operational security and attack sophistication. It can now be argued that their cyber capabilities rival those of Russia.”

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

The new threat landscape: COVID-19 creates new vulnerabilities, counter IR surges and more

COVID-19 has undoubtedly exposed new cracks in organizations' cyber defenses. But for the most part, the underlying methodologies behind the attacks we're seeing has remained relatively consistent.

So what's new?

First and foremost, COVID-19 has been accompanied by a surge in cyberattacks: more than half (53%) of all respondents encountered or observed an increase related to the pandemic.

Lukáš Hlavička, director of the Digital Forensics and Incident Response department at LIFARS, attributes this rise mostly to new spear phishing attacks. "The only difference is the pretext – related to COVID-19 – by which they get users to open the email."

He adds that most organizations weren't prepared for the majority of their employees to be working from home – and therefore don't have the capacity to protect networks in this new reality.

These insights align with our survey findings, which named remote access inefficiencies (52%), VPN vulnerabilities (45%) and shortage of available or skilled staff (36%) as the most daunting endpoint security challenges related to the pandemic.

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

What are the most daunting endpoint security challenges you have observed relative to the COVID-19 pandemic?

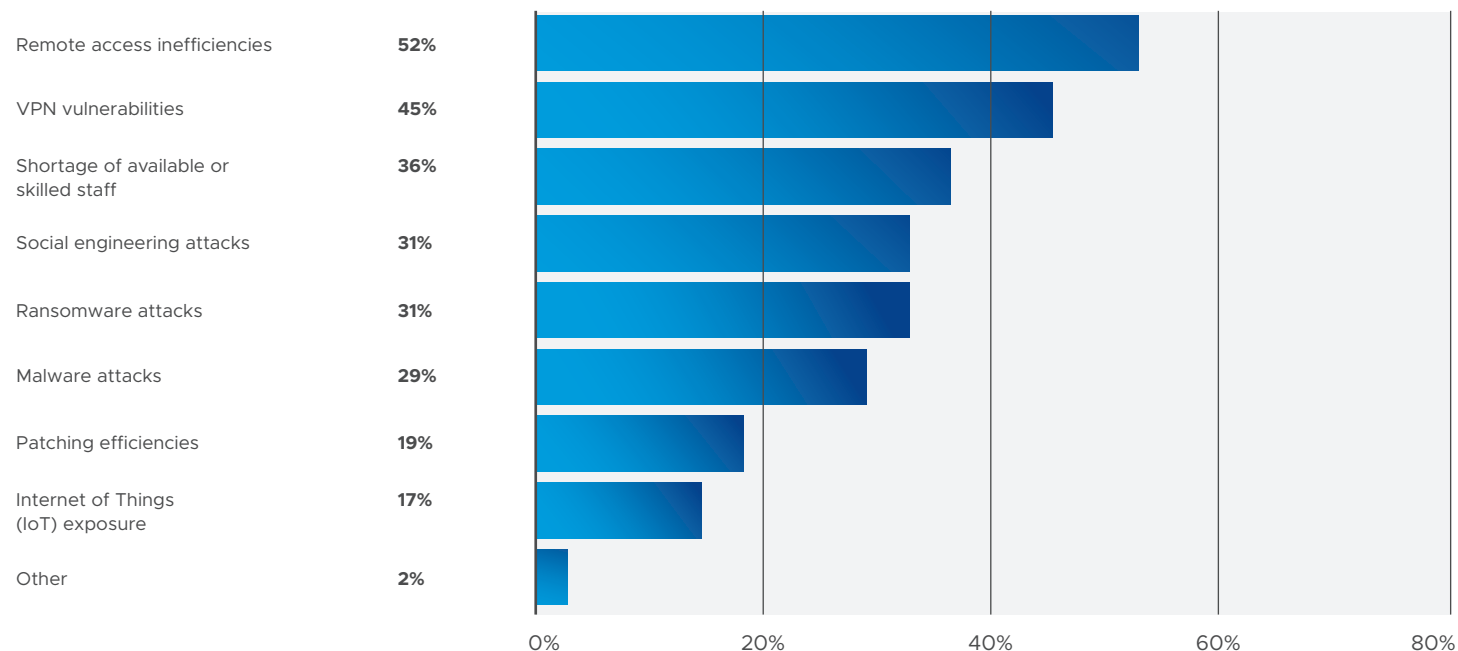


FIGURE 4: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

“Security teams now have to manage remote security configurations and provide real-time prevention rule updates to a slew of new, remote endpoints,” says Kellermann. “In the absence of a cloud infrastructure for security, how do you rapidly deploy additional security to users? Improve investigations and endpoint visibility? Track unwanted configurations? These are challenges they face regardless of COVID-19, but the stakes are now higher for these common challenges amid global disruption.”

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

VPNs, which many organizations rely on for protection, have become increasingly vulnerable amid COVID-19, according to more than 60% of respondents. As such, it may be cause for concern that the average update cycle for software patches and security configurations on VPNs tends to occur on a weekly (or less frequent) basis. Only 22% of respondents said VPN updates come daily – and Kellermann suggests even this might not be enough, primarily due to the explosion of traditional and fileless malware.

McElroy advises that, when it comes to VPNs, “You want your critical cases addressed within days, your high-level cases addressed within weeks and your mediums within a month. There’s an enormous amount of change management and testing that must happen when you roll out these patches, so you want to make sure you’re doing it right.”

As far as other new vulnerabilities go, IR professionals point to the use of IoT technologies, personal devices like iPhones and iPads, and web conferencing applications – all of which are

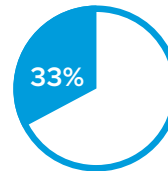
increasingly in professional use as work moves remote and the corporate perimeter breaks down. For instance, respondents said that 27% of incidents during the 90 days prior to the survey took advantage of IoT-related vulnerabilities.

“Last Christmas, the number one consumer purchase was smart devices,” says Kellermann. “Now they’re in homes that have fast become office spaces. Cybercriminals can use those family environments as a launchpad to compromise and conduct criminal conspiracies in professional organizations.”

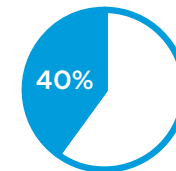
In other words, attackers are still island hopping – but instead of starting from one organization’s network and moving along the supply chain, the attack may now originate in home infrastructures. Like lateral movement, about a third of respondents saw an attack that used island hopping, 40% of which spread destructive malware in the process. What’s more, its use, like attacks more broadly, has been primarily aimed at the financial sector, where 50% of IR professionals who witnessed the method encountered it.

+60%

VPNs, which many organizations rely on for protection, have become increasingly vulnerable amid COVID-19, according to more than 60% of respondents.



Like lateral movement, about a third of respondents saw an attack that used island hopping.



Forty percent of attacks that used island hopping spread destructive malware in the process.

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

During the past 90 days, which industries have you seen targeted by cyberattacks?

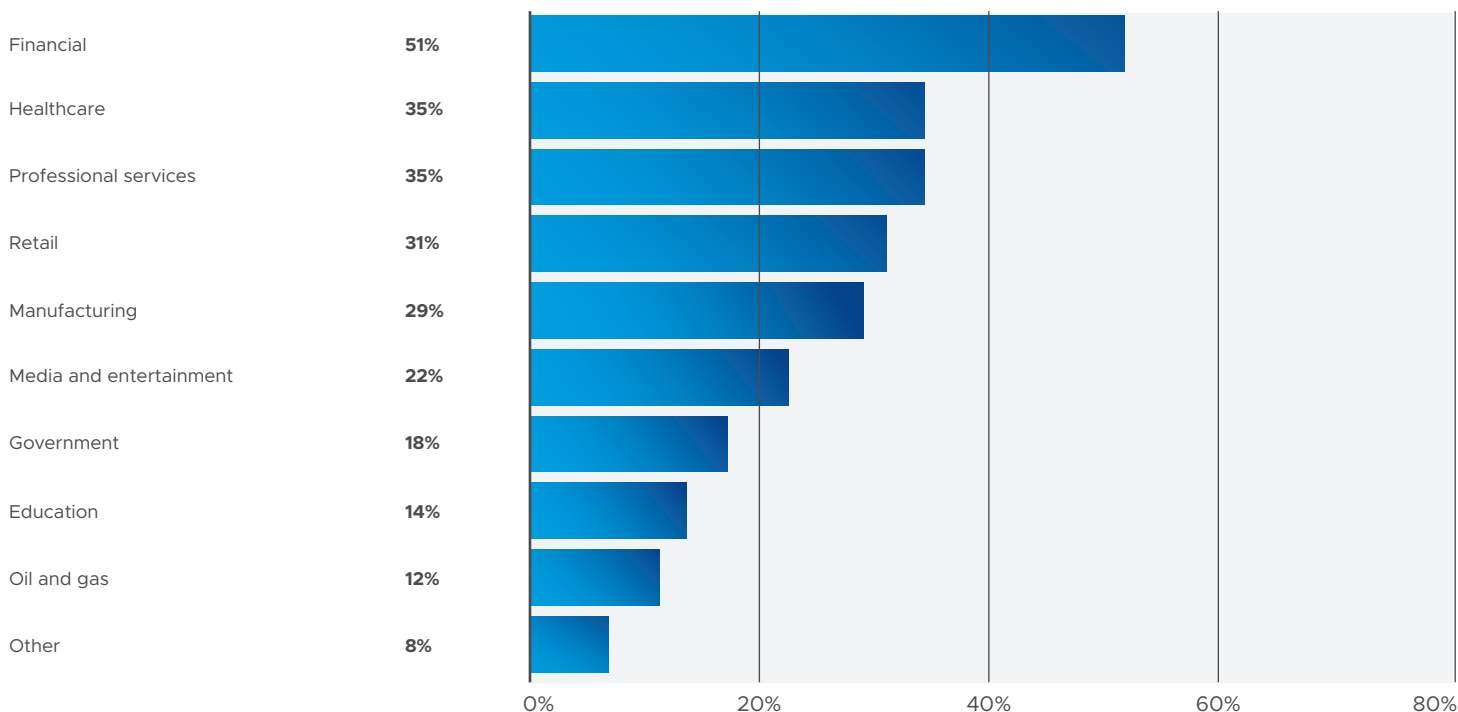


FIGURE 4: Multiple answers per participant possible. Percentages added may exceed 100 since a participant may select more than one answer for this question.

“It makes sense to use the brand of a financial organization to then target high-profile, high-net- worth customers,” says Kellermann.

According to our respondents, the financial industry was also the top priority for cyberattacks, with more than half (**51%**) having seen the industry targeted in the 90 days before they were surveyed. Healthcare (**35%**), professional services (**35%**) and retail (**31%**) were viewed as the next biggest targets.

Executive Summary	>
Key Highlights	>
The New Threat Landscape	>
The Evolving Roles	>
Looking Ahead	>
NTT DFIR Case Study	>
LIFARS Case Study	>
How to Fight Back	>

It doesn't help that today's attackers now move about systems in more clandestine ways. For instance, the Kryptik trojan, which is responsible for over 70% of attacks on the financial services sector of late, provides bad actors numerous access points and backdoors into a system. It can be persistent and difficult to detect, as it often deletes its executable file after running. And it can use trusted protocols to hollow out existing processes and penetrate the corporate environment even further via island hopping and/or lateral movement – also known as “lay of the land attacks.”

Kryptik is emblematic of the evolving threat landscape, where counter IR is on the rise (it increased 10% from our previous survey and was

seen in a third of incidents), lateral movement and island hopping remain difficult to detect and attacks take on an increasingly destructive nature (one in four respondents saw destructive attacks in half of all encountered incidents).

“We’ve gotten better at IR,” McElroy says. “So attackers have to obey that sophistication on our side now by doing counter IR, whether it’s remaining hidden to destroy logs, moving laterally to other parts of the infrastructure or conducting denial-of-service attacks. Evasion is built into the very fabric of malware now. To gain the upper hand, we’ve got to step it up on our end.”

+10%

Kryptik is emblematic of the evolving threat landscape, where counter IR is on the rise, increased 10% from our previous survey, and was seen in a third of incidents.

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

The evolving roles of security and IT teams

A simmering issue, which the current crisis will only aggravate, concerns the roles of IT and security teams in an organization and the risks posed by a lack of coordination between the two. In a recent report, nearly 80% of respondents described the relationship between these groups as negative. And 92% of respondents to our survey agreed that more collaboration would improve security and lessen cyber risk.

For the most part, however, IT teams still hold the reigns: Even when it comes to threat hunting, more respondents said the IT team remains the primary decision-maker.

“It’s been a failure of corporate governance for a while now,” Kellermann says. “IT teams and CIOs

are still superior to security teams and CISOs. It’s like putting the offensive coordinators in charge of defense.”

Our survey suggests the tide is turning, however, as skill sets and tools evolve – and as boards begin to seek more strategic alignment. To that end, when asked which initiatives will help drive the most collaboration between IT and security teams, our respondents named the following as the top three:

1. Establishing a consolidated strategy with unified metrics and goals (61%)
2. Modifying reporting structures to streamline communications upstream (47%)
3. Integrating platforms and solutions for seamless sharing of information between teams (47%)

In your opinion, which team in an enterprise is currently primarily responsible for threat hunting/incident response and endpoint security?

	Threat hunting/ incident response	Endpoint security
IT team is the primary decision-maker	(20) 41%	(19) 40%
Security team is the primary decision-maker	(19) 39%	(17) 35%
IT and security teams share responsibility	(10) 20%	(12) 25%
Total	49	48

In your opinion, in the next three years, which team in an enterprise will be primarily responsible for threat hunting/incident response and endpoint security?

	Threat hunting/ incident response	Endpoint security
IT team is the primary decision-maker	(14) 29%	(16) 33%
Security team is the primary decision-maker	(22) 46%	(22) 45%
IT and security teams share responsibility	(12) 25%	(11) 22%
Total	48	49

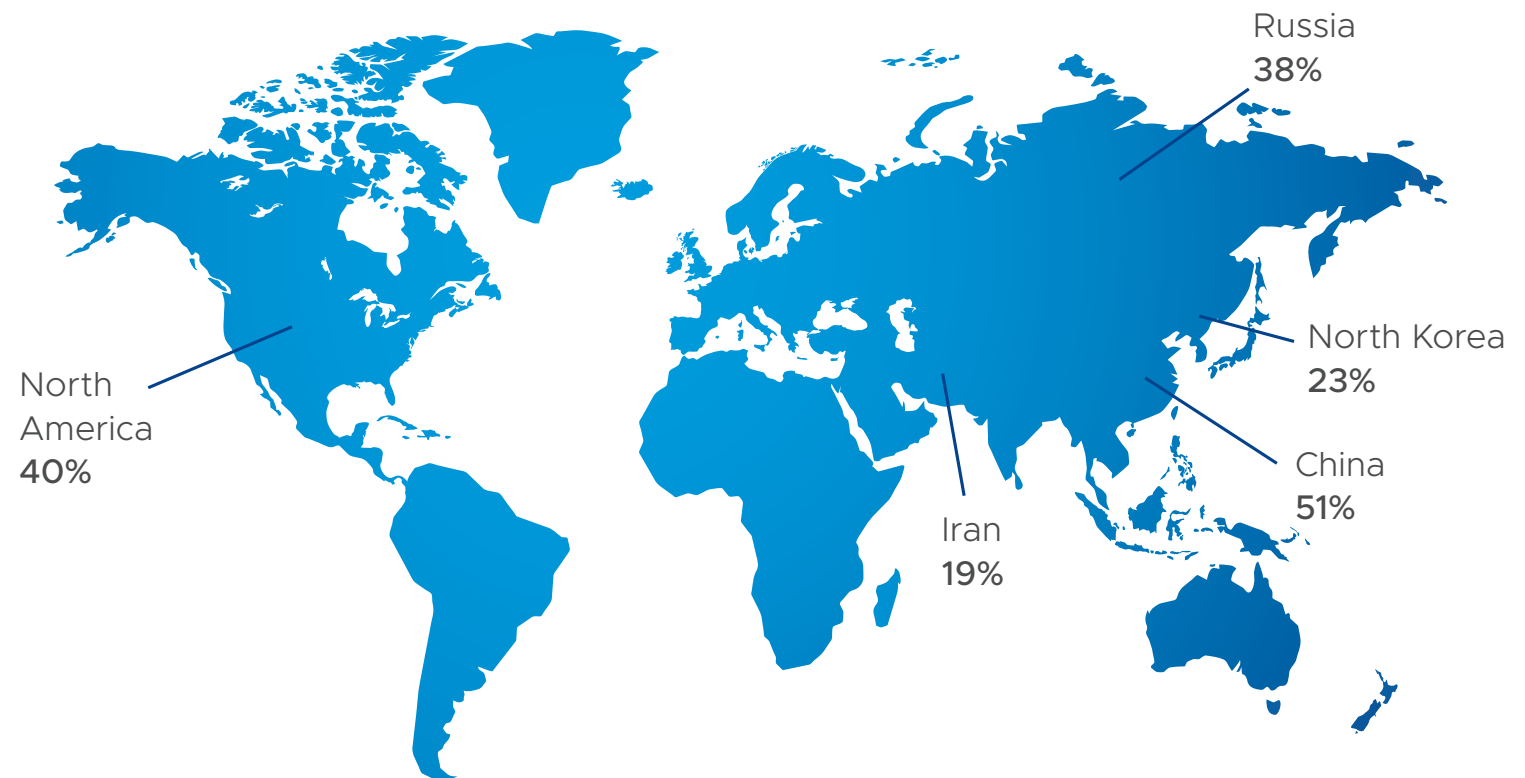
[Executive Summary >](#)[Key Highlights >](#)[The New Threat Landscape >](#)[The Evolving Roles >](#)[Looking Ahead >](#)[NTT DFIR Case Study >](#)[LIFARS Case Study >](#)[How to Fight Back >](#)

Looking ahead

As the initial shock of COVID-19 subsides, we should expect organizations to firm up their defenses against new vulnerabilities – whether it's addressing staff shortages, integrating endpoint technologies, aligning IT and security teams or adapting networks and employees to remote work.

What won't dissipate are burgeoning geopolitical tensions from China and Russia, particularly as we near the 2020 presidential election. Nearly half of all respondents said these tensions were leading to a rise in destructive attacks.

During the past 90 days, which countries have you seen cyberattacks from?



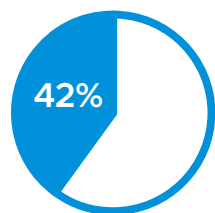
[Executive Summary >](#)[Key Highlights >](#)[The New Threat Landscape >](#)[The Evolving Roles >](#)[Looking Ahead >](#)[NTT DFIR Case Study >](#)[LIFARS Case Study >](#)[How to Fight Back >](#)

“The Chinese regime is hitting an existential moment in their history,” Kellermann says. “COVID-19 has caused them to lean on the soft power of cyber to maintain stability within borders and disrupt adversaries. Couple this with the ongoing trade war, and you’ve got a real driver for hostility playing out across cyberspace.”

Emerging attack types are on the horizon as well. Forty-two percent of respondents, for instance, said that cloud jacking would “very likely” become more common in the next 12 months, while 34% said as much of access mining. Mobile rootkits, virtual home invasions of well-known public figures and Bluetooth low energy attacks were among the other attack types respondents saw coming to the fore in the next year.

Speaking on mobile rootkits, for instance, McElroy says, “We know nation-states are using them, but now that executives are working on iPads and iPhones, we should expect more to join in. They have time on their hands to develop these techniques in ways they haven’t had before.”

These new methods, in tandem with a surge in counter IR, destructive attacks, lateral movement and island hopping, make for a perilous threat landscape. But with the right tools, strategies, collaboration and staff, IR teams can handle the threat. They’ve met many of these challenges before, and there’s no reason why they shouldn’t be able to again.



Forty-two percent of respondents said that cloud jacking would “very likely” become more common in the next 12 months.

Executive Summary >

Key Highlights >

The New Threat Landscape >

The Evolving Roles >

Looking Ahead >

NTT DFIR Case Study >

LIFARS Case Study >

How to Fight Back >

Rooting out a persistent, evasive, and destructive DoublePulsar attack

At a Fortune 500 organization with over 100 locations around the world, the security notification came in: several Server Message Block (SMB) DoublePulsar alerts suggesting a possible compromise within the company's environment. The malware, leaked in 2017 by Shadow Brokers, targets Windows, opening a backdoor through which more malware can be loaded onto infected systems – systems that can then be used to distribute and launch attacks on others.

The company's security team suspected one or more endpoints were compromised but, because the alerts were intermittent, they were unable to determine which systems. To minimize further impact, the team set up a firewall rule to terminate any Server Message Block Version 1 (SMBv1) network sessions propagating the malicious traffic and used the Carbon Black Cloud platform to quarantine endpoints associated with said traffic.

From there, the organization activated their Incident Response Plan and engaged the NTT Digital Forensics Incident Response (DFIR) team to aid in the investigation.

To that end, the NTT DFIR team immediately deployed Carbon Black's EDR technology to obtain remote intrusion analysis capabilities and visibility throughout the network. Once it was deployed, NTT DFIR used Carbon Black's Live Response features to perform threat hunting analysis and identify the malicious

machine. They found that the attacker had used PowerShell scripts containing NET USE commands and credential-stealing malware to propagate itself via SMB protocols.

NTT DFIR also determined that the malicious attack was intermittent because whenever the virus reached a sinkholed domain, it would not attempt to propagate across the network. Yet when it did reach a sinkholed domain, the virus would attempt to compromise other SMBv1 devices and access network shares to detonate WannaCry ransomware.

The attacker used SMB DoublePulsar, NetBIOS null session, and SMB: User Password BruteForce attacks to further infiltrate the organization's network. Once discovered, the attacker sought to adversely impact the business via the detonation of WannaCry ransomware. Finally, NTT DFIR discovered the original compromised system (located in China) was modified using a pirated version of Microsoft Windows, which functioned without IT security controls (e.g., antivirus) and contained several other malicious hacker tools.

Following this investigation, NTT DFIR recommended the infected machine be wiped, re-imaged with an official version of Microsoft Windows and have IT security controls installed.

In addition, NTT DFIR advised the organization to consider accelerating the implementation of a network access control solution. This way, only authorized devices could be connected to their internal network, thereby preventing this event from occurring in the future and satisfying the criteria of the company's secure device policy.

[Executive Summary >](#)[Key Highlights >](#)[The New Threat Landscape >](#)[The Evolving Roles >](#)[Looking Ahead >](#)[NTT DFIR Case Study >](#)[LIFARS Case Study >](#)[How to Fight Back >](#)

LIFARS Case Study

The adversary had free reign over a fintech's networks – until Carbon Black came in

You know it's a real emergency when the call comes on a Saturday night.

Nearly every server at a large fintech organization had been compromised and encrypted, malware was spreading across the network and the IT team in charge had no control over the situation. Access to critical data was at stake.

Then the ransomware came, spreading laterally via RDP, domain accounts, WMI. When the IR team finally got called in Monday morning, they discovered the attacker had what might as well be a golden ticket: the ability to get access to any user and traverse the system architecture at will. Even a kill switch proved unsuccessful.

By using VMware Carbon Black technology, the IR team gained the visibility it needed to see that the ransomware was deployed by the malware Dridex. Yet this adversary's brand was particularly evasive: It ran analyses at various endpoints to see if it was being analyzed; if it thought it was, it didn't deploy any ransomware function. Whenever the IR team blocked its access, the adversary found access to machines not yet protected by CB and tried to obtain new passcodes and credentials to then redeploy itself throughout the infrastructure.

Using CB, the IR team could run an in-depth analysis of a malware sample, giving them indicators of what the malware wanted to do next. From there, they created a "vaccine" that could be deployed via CB's API to every endpoint in the organization.

When all was said and done, the organization had suffered over 63,000 single infections, with some computers infected multiple times. But with CB deployed, the IR team remediated the situation, getting everything secure and up and running in just 72 hours – before another Saturday night could be ruined by a cyber emergency.

Executive Summary	>
Key Highlights	>
The New Threat Landscape	>
The Evolving Roles	>
Looking Ahead	>
NTT DFIR Case Study	>
LIFARS Case Study	>
How to Fight Back	>

How to fight back

Next generation cyberattacks – with adversaries increasingly working to maintain persistence on systems – call for next generation IR, especially as corporate perimeters across the world break down. Here are five steps security teams can take to fight back.

01 Gain better visibility into your system's endpoints. Doing so can empower security teams to be proactive in their IR – rather than merely responding to attacks once they come, they can hunt out prospective threats. This is increasingly important in today's landscape, with more attackers seeking to linger for long periods on a network and more vulnerable endpoints online via remote access.

02 Establish digital distancing practices. People working from home should have two routers, segmenting traffic from work and home devices. They should have a room free of smart devices for holding potentially sensitive conversations. And they should restrict sensitive file sharing across insecure applications, like video conferencing tools.

03 Enable real-time updates, policies and configurations across the network. This may include updates to VPNs, audits or fixes to configurations across remote endpoints and other security updates – even when outside the corporate network. “It's important to keep in mind the security architecture when making these changes,” Hlavička adds. “Otherwise, things get changed without having the proper controls in place to react.”

04 Remember to communicate. Now more than ever, organizations need to prioritize change management and maintain clear lines of communication – about new risk factors (spear phishing, smart devices, file-sharing applications, etc.), protocols and security resources. Security teams should also hold drop-in hours for any questions and/or hygiene checks.

05 Enhance collaboration between IT and security teams – and make IT teams more cybersecurity savvy. As noted, 92% of IR professionals agree that a culture of collaboration between IT and security teams will improve enterprise security and response to cyber risks. This is especially true under the added stress of the pandemic. Alignment should also help elevate IT personnel to become experts on their own systems, McElroy notes, whether it's training them to threat hunt on a Windows box or identify anomalous configurations on certain SaaS applications.

Methodology

VMware Carbon Black conducted an online survey about trends in incident response in April 2020. Forty-nine IR professionals from around the world participated. Percentages in certain questions exceed 100% because respondents were asked to check all that apply. Due to rounding, percentages used in all questions may not add up to 100%.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com/company. VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and other jurisdictions.



Join us online:

