Carbon Black.

GLOBAL
INCIDENT RESPONSE
THREAT REPORT

The Ominous Rise of "Island Hopping" & Counter Incident Response Continues

Advanced Cyberattacks Are Evolving as Attackers Target Supply Chains and Battle Back Against Cybersecurity Teams

APRIL 2019

Executive Summary

During his NBA career, Magic Johnson made everyone around him better: his teammates, obviously, but also his opponents, who were forced to step up their games if they wanted to keep up.

Cybercrime certainly isn't basketball — the stakes are higher, your jump shot doesn't matter — and yet the principle remains the same. As incident response (IR) teams and their vendors raise the defensive bar, adversaries adapt in kind.

According to the world's leading IR professionals, increasingly sophisticated attacks involving instances of "island hopping," counter incident response (IR), and lateral movement within a network are quickly becoming the new normal. Tom Kellermann, Carbon Black's chief cybersecurity officer, concurred, noting that the trend signals a cybercrime wave that's continuing to evolve.

"Attackers are fighting back. They have no desire to leave the environment. And they don't just want to rob you and those along your supply chain. In the parlance of the dark web, attackers these days want to 'own' your entire system," Kellermann said.

While financial and healthcare organizations continue to be top targets for these attacks, the manufacturing industry has seen a steep rise in incidents as cybercriminals aim to steal valuable IP. These motives and methods may very well reflect roiling geopolitical tensions — be it uneasy trade relations with China or what looks to be a new nuclear arms race with Russia — as nation states seek competitive advantage.

To stay abreast of the current attack landscape and to quantify the latest attack trends seen by leading IR firms, **Carbon Black is publishing its third Global Incident Response Threat Report since introducing it in July 2018.** Aggregating qualitative and quantitative input from 40 Carbon Black IR partners, this report aims to offer actionable intelligence for business and technology leaders, fueled by analysis of the newest threats and expert insights on how to stop them.

Carbon Black has one of the most robust IR partner communities in cybersecurity. These 100+ IR partners conducted more than 500 response engagements in 2018 and continue to use Carbon Black solutions in more than one engagement per day on average. The insights from this report chronicle Carbon Black partners' experiences during these critical engagements.

OF TODAY'S ATTACKS LEVERAGE
ISLAND HOPPING

Carbon Black.

Among the Key Findings:

1. **Exactly half (50%) of today's attacks leverage "island hopping."** This means that attackers are after not only your network but all those along your supply chain as well.

2. **More than half of survey respondents (56%) encountered instances of counter IR in the past 90 days. 87%** have seen this take the form of **destruction of logs**, while **70%** witnessed **evasion tactics**.

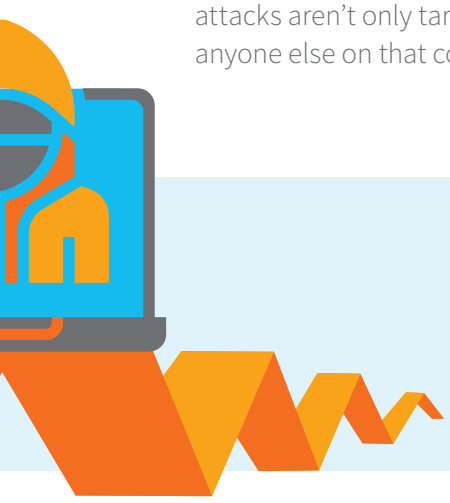
3. **70% of all attacks now involve attempts at lateral movement**, as attackers take advantage of new vulnerabilities and native operating system tools to move around a network.

4. **Nearly a third (31%) of targeted victims now experience destructive attacks —** an alarming byproduct of attackers gaining better and more prolonged access to targets' environments.

5. **The financial and healthcare industries remain most vulnerable to these attacks,** but the threat to **manufacturing** companies has grown significantly. In the past 90 days, **nearly 70% of all respondents** saw attacks on the **financial** industry, followed by **healthcare (61%)** and **manufacturing (59%, up from 41% last quarter).**

"Island hopping" gets more prevalent — and dangerous

As stated above, half of today's attacks now leverage "island hopping." That means half of today's attacks aren't only targeting one organization — they're also intending to access the networks of anyone else on that company's supply chain.



"In the parlance of the dark web, attackers these days want to 'own' your entire system."

— Tom Kellermann, Carbon Black's chief cybersecurity officer

IN WHICH INDUSTRIES DID YOU ENCOUNTER ISLAND HOPPING?

(Respondents were given the choice to select all that apply)

FINANCIAL	47%
MANUFACTURING	42%
RETAIL	32%
HEALTHCARE	21%
GOVERNMENT	16%
PROFESSIONAL SERVICES	16%

Carbon Black.

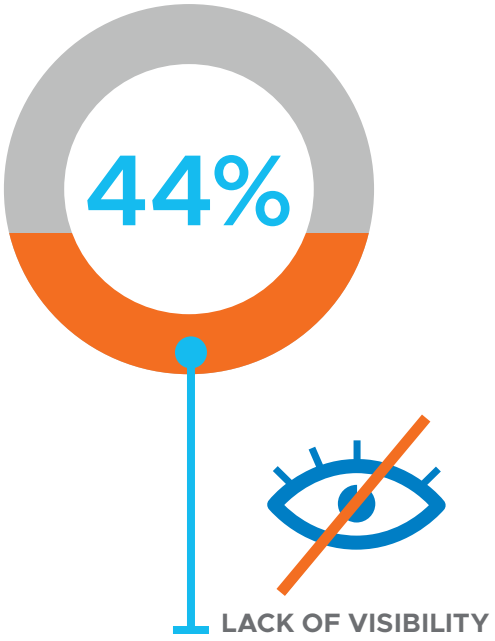
"At this point, it's become part and parcel of a cybercrime conspiracy," said Kellermann. "They're using their victim's brand against customers and partners of that company. They're not just, say, invading your house — they're setting up shop there, so they can invade your neighbors' houses too."

The industries in which our respondents encounter "island hopping" most frequently are **financial (47%), manufacturing (42%)**, and **retail (32%)**. Worrisome, too — because of their access to confidential client work and IP — are **professional services firms (16%)**.

As with all cybercrime, geopolitical tensions likely manifest in this growing threat, particularly when it comes to financial and manufacturing organizations. Amid world-wide trade negotiations, evolving economic sanctions, and an ever-globalizing marketplace, nation state actors are seeking any competitive advantage they can get.

"Going after manufacturing companies for IP purposes reduces R&D costs for designing everything from

GENERALLY SPEAKING, WHAT IS THE TOP BARRIER TO EFFECTIVE INCIDENT RESPONSE IN THE INDUSTRY RIGHT NOW?



Carbon Black.

airplanes, to cell phones, to high-grade weapons," said Ryan Cason, director of partner solutions at Carbon Black. "It allows them to get to market quicker, at a cheaper price point, to the detriment of their victim."

Consequently, we saw a steep rise in **intellectual property theft** as an attacker's end goal this quarter, with **22% of respondents** saying this was the case **(as opposed to 5% last quarter)**. Unsurprisingly, **financial gain** remains the most common end goal, at **61%**.

Why are organizations so vulnerable to "island hopping?" It comes down to a **lack of visibility**, which our respondents **(44%, up 10% from last quarter)** named the top barrier to incident response.

"More often than not, the adversary is going after the weakest link in the supply chain to get to their actual target," said Thomas Brittain, who leads Carbon Black's Global IR Partner Program. "Businesses need to be mindful of companies they're working closely with and ensure that those companies are doing due diligence around cybersecurity as well."

"There's an implicit trust placed on a partner's communications," added Kellermann. "And those communications are often only governed by DLP, which has no capacity to discern when your organization is the cause of pollution via fileless malware. Most east-west monitoring is done by DLP solutions and firewalls when it needs to be done from endpoints."

THREE FORMS OF "ISLAND HOPPING"

As "island hopping" becomes a more persistent threat, the technique has taken on new forms. Here are the three that organizations should be keeping an eye out for right now.

1 **Network-based "island hopping."** This is what we typically think of when we think "island hopping" — an attacker leveraging your network to "hop" onto an affiliate network. Of late, this has often taken the form of targeting an organization's managed security services provider (MSSP) to flow through their connections.

2 **Websites converted into a "watering hole."** In the past 90 days, 17% of respondents saw a victim's website converted into a "watering hole," a technique aimed at ensnaring a victim's customers and partners. Kellermann noted, "It's the greatest way to hijack a brand, and, as such, organizations need to make this a brand protection issue. CMOs have to have their own cybersecurity strategy in place as it relates to their digital marketing footprint."

3 **Reverse Business Email Compromise (BEC).** This is a new trend, occurring primarily in the financial sector, wherein attackers take over the mail server of their victim company and leverage fileless malware attacks from there to those who trust it. Some are calling it the modern bank heist.

CASE STUDY: An ATM Cash-Out Scheme Stopped in Its Tracks

You know it's serious when the Secret Service calls.

But that's exactly what happened to a regional financial services company this past year. The tip? There's an ATM cash-out scheme on the horizon — and we think the attackers already have access to your network.

They were right. Attackers had gotten into the bank's wire transfer and fraud monitoring systems, where they were able to decrease controls designated to make sure customers can't transfer large amounts of money too quickly. They were in place to clone accounts, make fake ATM cards, and move those aforementioned large amounts of money from the good accounts to the bad — at which point hired foot soldiers would go to ATMs and withdraw and withdraw until the levee went dry.

BTB Security's IR team was called in to stop the bad guys before it was too late. They set out on a fact-finding mission: preserving and reviewing evidence, analyzing system devices and application logs, and, with the help of Carbon Black, establishing active monitoring on all servers and endpoints.

CB Response ultimately gave BTB the visibility they needed to find the source of the breach in less than five hours, using various data sets to trace the infected server back to a workstation that had received a phishing email just before the network was compromised.

With this information in hand, BTB could use CB Response and other tools to build up a picture of the incident: essentially, an organized crime group from the Eastern bloc had gained persistent connections to the bank's networks, leveraging WMI and PowerShell scripting to gain command and control of various systems as well as the ability to move laterally within the environment. It seemed likely, too, that the hackers had purchased access on the dark web from a group based in the Asia-Pacific.

At the behest of the Secret Service, BTB didn't turn on the lights on the attackers right away — instead, they instituted some tight controls but let the hackers remain inside long enough for law enforcement to obtain prosecutorial evidence. The information they helped procure gave the federal government and other industry players more insight into a scheme with growing prevalence.

It might have all been prevented if the company had no-blind-spot monitoring in place, as well as fast incident response once the problem was identified. Rest assured they are prepared not to make those mistakes again. And hopefully they won't be getting any more calls from the Secret Service either.

BTB SECURITY

Carbon Black.

Counter-Incident Response Gets More Sophisticated — And Destructive

To outwit defenders, attackers are finding new ways to stay inside their victims' networks. In the past 90 days, **56% of respondents** have encountered instances of attempted **counter IR** — **up 5%** from last quarter alone. Again, financial and manufacturing are top targets, with **36% of IR professionals** seeing these instances within **financial organizations** and **27%** in **manufacturing**.

A full **70% of respondents** said counter IR took the form of **evasion tactics.** As Brittain described it, "An attacker is going to turn off antivirus, firewalls, anything that's going to send a trigger upstairs, because the longer they have to achieve their goal — whether it's lateral movement, 'island hopping' further up the supply chain, or data collection — the better chance they'll have for success."

Of course, these tactics are reflective of the growing prominence of lateral movement in a network, which now occurs in **70% of incidents**. What's more, nearly **40% of respondents** said **lateral movement** took place in **90% of attacks or more**.

DURING THE PAST 90 DAYS, HAVE YOU ENCOUNTERED INSTANCES OF ATTEMPTED COUNTER-INCIDENT RESPONSE?

RESPONDENTS ANSWERING YES HAVE INCREASED BY **5%** EACH QUARTER

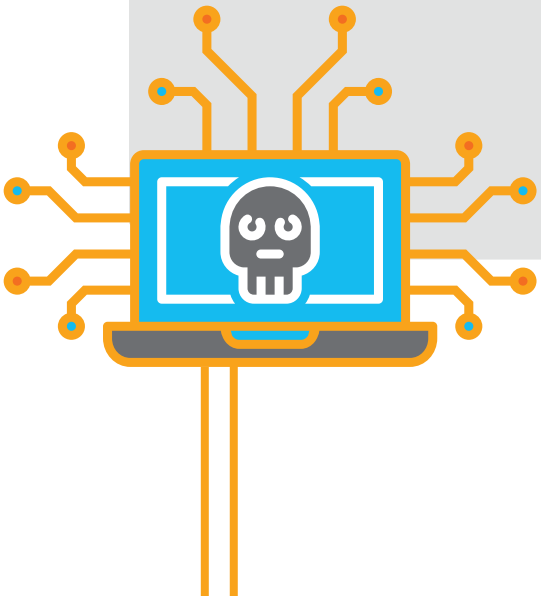
Carbon Black.

IN WHICH INDUSTRIES DID YOU ENCOUNTER COUNTER-INCIDENT RESPONSE?

(Respondents were given the choice to select all that apply)

FINANCIAL	36%
MANUFACTURING	27%
HEALTHCARE	24%
EDUCATION	23%
PROFESSIONAL SERVICES	23%
RETAIL	23%
MEDIA AND ENTERTAINMENT	18%
GOVERNMENT	14%

Carbon Black.



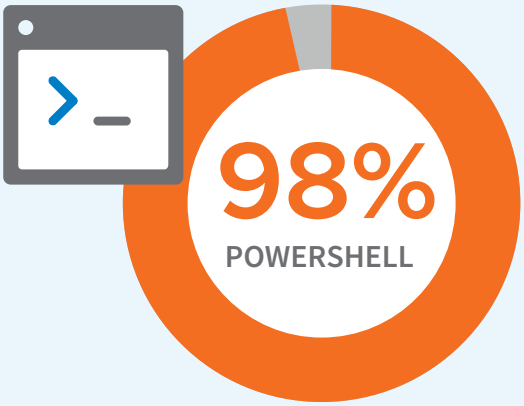
It should come as no surprise that most attackers are taking advantage of **PowerShell (98% of respondents said as much)** and **WMI (83%)**. But as defenders get better at monitoring these tools, adversaries have increasingly turned toward **process hollowing (up to 56% from 38% last quarter)** and **script hosts (40%)**. These methods help disguise attackers' methods and are harder to detect.

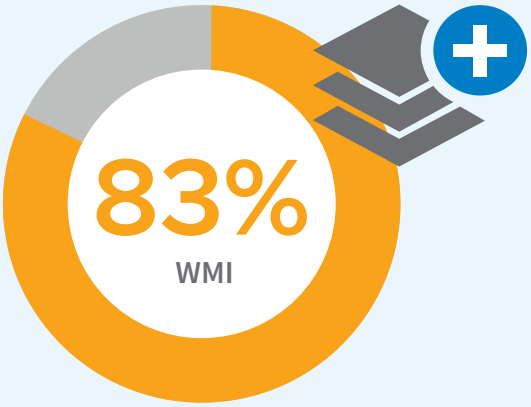
Brittain explained: "Process hollowing is an in-memory attack. It's the ability to get on a system, take control of a legitimate process, hollow it out, and replace it with malicious code. Script hosts, meanwhile, allow them to write their own code directly into memory (that's not executable) — which can bypass most defense systems."

As with "island hopping," visibility is key: "Having an endpoint detection and response (EDR) tool on your endpoints can help you detect when a scripting host is called and can also tell you when an application injects itself into another one," said Cason.

> "Process hollowing is an in-memory attack. It's the ability to get on a system, take control of a legitimate process, hollow it out, and replace it with malicious code."
>
> — Thomas Brittain, lead, Carbon Black's Global IR Partner Program

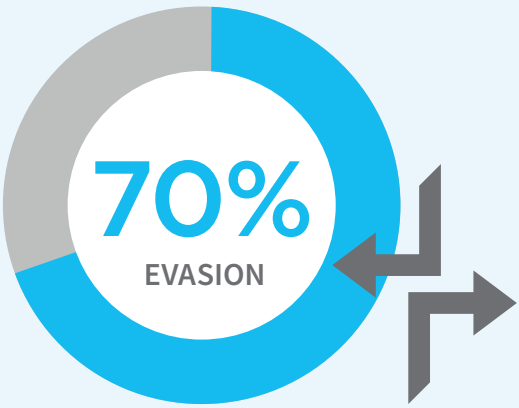
WHICH DUAL PURPOSE TOOLS DO YOU SEE HELPING TO FACILITATE LATERAL MOVEMENT FOR ATTACKERS?





WHAT FORMS OF COUNTER-INCIDENT RESPONSE HAVE YOU SEEN?

(Respondents were given the choice to select all that apply)



Carbon Black.

Troublingly, even if you kick an attacker out of a system these days, the attacker will often have methods for lurking around and eventually getting back in undetected. For instance, **40% of respondents** encountered instances of **secondary C2** used on a sleep cycle. What's more, the increased use of steganography — essentially, hiding data in other content types like images, videos, and network traffic — means that these attackers may be hanging out in a network without IR teams even knowing they're there.

While evasion tactics are undoubtedly vital in counter IR, the top form, according to **87% of our respondents,** is destruction of logs — a **15% increase from last quarter**. "It's a great way for an adversary to hide their tactics," Brittain said. It follows that **75% of respondents** said event logs are the most valuable artifact an IR team needs to collect during an investigation — it's crucial, while conducting IR, to preserve the environment.

STEGANOGRAPHY —

the hiding of data in other content types such as images, videos, and network traffic, — continues to play a role in modern attacks in several forms. However, most uses in malware can be divided into two broad categories:

1. **Concealing the actual malware contents itself**

2. **Concealing the command and control communications channel**

Embedding multiple content types within a single file to evade detection has been a common technique for some time. But more sinister versions of this tactic have been observed of late, wherein attackers covertly embed malware code payloads in image files. Carbon Black, for instance, recently documented an attacker's efforts to embed malicious code into a set of PNG files, which were then compiled into a legitimate application with a function that would extract and drop the malware onto the system.

As for command and control protocols, steganography is often used to read content from image files available via sharing and social media sites. The network traffic and associated images hide in plain sight among the other legitimate uses of such services. Additionally, tunneling C2 communications in existing protocols such as DNS and HTTP by embedding information in unused or uncommon fields is also often seen in modern malware.

CASE STUDY: Stopping Sophisticated Cyber Spies in Their Tracks

These days, cyberattacks can be a lot like a bad case of bed bugs. You can clean your clothes, replace your sheets, toss out your mattress — and still wake up a few mornings later with bites.

Take DarkMatter's recent client engagement. They were called in to perform a post-incident compromise assessment two months after an organization's internal IR team had (supposedly) cleared the scene. In the process, CB Response allowed DarkMatter to identify what the previous IR team's SIEM solution had not: a PowerShell execution in memory on the organization's domain controller, which was identified as an implementation of OilRig-attributed malware.

OilRig, a cybergroup thought to be of Iranian origin, had established additional backdoor footholds in the environment — using techniques learned from the Russian group APT29. Their goal? Espionage. It makes sense they'd want to stick around undetected.

In the attack's initial phase, OilRig had launched a successful spear phishing attack, after which they leveraged built-in Windows functionalities, queries, and tools to perform reconnaissance and send two more successful spear phishing emails. In this second phase, the domain controller was the target, as was executing PLINK (a tool for remote port forwarding) on an application server to gain additional footholds and exfiltrate data.

With the visibility and unfiltered data gained through CB Response, DarkMatter's analysts could do what they do best: hunt threats. Remediation was swift. This time, it was thorough.

But as geopolitical tensions continue to mount and attackers develop more sophisticated techniques, we should expect a growing number of incidents like these in the future. To fight back, IR teams need SIEM solutions that do more than focus solely on Windows event logs (as this organization's did). Rather, they need solutions that integrate core network logs as well as detection systems that are enhanced and tuned to avoid alert fatigue.

At the end of the day, full visibility is the first step in completely ridding an environment of an attacker — whether they're a cybergroup like OilRig or a particularly nasty case of bed bugs.

DARKMATTER
SMART AND SAFE DIGITAL

Carbon Black.

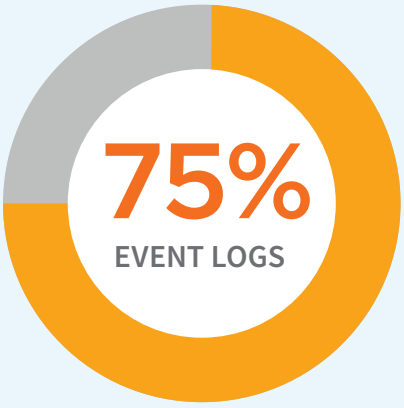
A New Set of Best Practices in IR

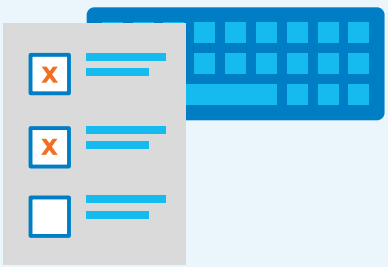
Without prior planning, infrastructure, and best practices in place, IR can go terribly, terribly wrong. One IR professional related this horror story:

"At a college whose network had been compromised, an attacker got into the IR team's systems. They started erasing their timeline, their response plan, even calling them out in the notes during the incident. The problem was that the IR team was using the same systems that had been compromised — the same email accounts, the same notebook, the same OneDrive — all because they didn't have the infrastructure in place to do IR the right way."

In today's cybercrime landscape, IR teams and the organizations they work with need to not only come prepared but be proactive, becoming threat hunters who can identify areas of vulnerability before a full-on breach.

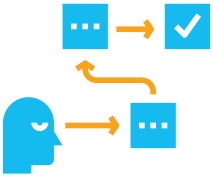
WHAT IS THE MOST VALUABLE ARTIFACT YOU NEED TO COLLECT DURING AN IR INVESTIGATION?





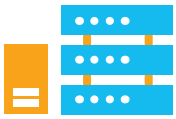
Carbon Black.

Here Are 5 IR BEST PRACTICES to Keep Top of Mind:



1 **Have a backup plan for setting up a new operating environment** — and make sure it's one you can get online in a few hours. As one IR professional said, "It's really quick to set up a new Office 365 system, but you need to have a playbook in place to do so, plus established lines of communication between the IR team and their client."

2 **Don't turn on the lights right away.** That is, don't immediately terminate the command and control system, and don't immediately let the adversary know you're watching them. To observe lateral movement and isolate targeted systems, being clandestine is key. Having EDR capabilities on all endpoints is also vital.



3 **Store data.** You need to store 30 or more days of data from all endpoints to preserve the environment and combat the destruction of logs that has become so prevalent. Cordon off a protected, central source that only you can access.

4 **Bring down the noise.** New technologies mean organizations and IR teams can collect (and monitor) more data than ever before. Alert fatigue, according to IR professionals, is real. So to detect attackers, it's crucial this data is contextualized. One IR professional suggests that, rather than working top-down with an overwhelming number of alerts, you need to build up rules manually. This means cross-referencing alerts against a given organization's threat profile, as well as their specific environment and mission, and then aligning those contexts with various watchlists (e.g.; the MITRE ATT&CK framework).

5 **Rebuild the environment from scratch and augment existing capabilities with EDR.** So, as one IR professional said, "If you get reinfected, we'll have the spotlight, the tapes, and the analysis of the root cause."

Carbon Black.

CASE STUDY: When Ransomware Strikes a Nonprofit

No matter how diligent you may be, the slightest of human errors gone undetected can leave your organization vulnerable to attack.

That's where a nonprofit got in trouble recently. An improper firewall change exposed one of the organization's servers, allowing an attacker to guess the correct user name/password combination for an administrator account and gain a foothold into the internal network. From there, they deployed ransomware to target available network shares for encryption and leverage the nonprofit's servers to extract money. Without proper change controls in place — and because the number of IP address alerts made it hard to filter out the noise — the firewall misconfiguration went unseen, and the attacker gained access.

Once they noticed the file encryption, they could trace it back to the compromised server, shut it down, and correct the firewall change. Even though the encryption stopped at that point, Optiv was brought in to make sure nothing else had happened and to produce a report that could facilitate effective remediation.

Luckily, the customer had CB Response deployed to their entire environment. Since the ransomware encrypted much of the traditional forensic evidence, CB Response played a crucial role in collecting a wide breadth of data — including event logs, executable and resource files, as well as file, network, and process activity.

At the same time, Optiv could leverage CB Response's high-fidelity alerts, feeds, and open-source automation scripts to review, triage, and investigate available data efficiently.

For instance, CB_Sensor_Dump, CB_Feeds_Dump, and CB Alerts provided Optiv with organized CSV exports from myriad sources. Concerning items could then be queried via the CB Response API to pull and drill down on relevant data, as well as cross-checked against outside threat intelligence sources. For example, Optiv could correlate network connections against events on other network hosts to identify if any lateral movement had occurred. In addition to these tactics, Optiv also used CB Response's Live Response feature to pull various artifacts and logs from endpoints without resorting to more time-consuming "dead-box" forensic imaging methods.

With CB Response, Optiv could confidently confirm that no additional compromise or lateral movement had occurred. They did so in short order without leaving the client in limbo about the state of their network. And they produced an extensive report that will help the organization prevent similar incidents in the future.

OPTIV

Carbon Black.

Conclusion: A Dangerous New Wave of Cybercrime

The growing prevalence of "island hopping," counter IR, and lateral movement is ushering in a new wave of dangerous cybercrime — particularly in the financial, healthcare, and manufacturing sectors.

These methods aren't only effective in financial theft, espionage, and data collection. They abet attackers in being outright destructive. An alarming 30% of our respondents have seen destructive or integrity attacks on targeted networks in the past 90 days.

Nation states in the grip of geopolitical conflict could be behind this new wave of attacks, but there are also terrorist groups, organized crime, and others who have gained prominence with the help of shadow brokers selling tools and information on the dark web. There are a growing number of bitcoin schemes in the financial sector that disguise a broader transfer of funds, a trend of reverse business email compromise attacks, and, as always, the specter of cyberattacks manifesting themselves in the physical world — be it attacks on hospital systems or IP theft that contributes to what might be a new nuclear arms race with Russia.

Even as we become more adept defenders, attackers are doing everything they can to stay out front. They're developing and sharing new techniques, exploiting new vulnerabilities, and finding new ways to remain invisible in a network to "own" the entire system.

As our adversaries seek to wreak havoc, businesses and IR teams need to stay on the cutting edge if we want to fight back with success.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint security and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

"Businesses need to be mindful of companies they're working closely with, and ensure that those companies are doing due diligence around cybersecurity as well."

— Thomas Brittain, lead, Carbon Black's Global IR Partner Program.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com