Carbon Black.

QUARTERLY
INCIDENT RESPONSE
THREAT REPORT

Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections

NOVEMBER 2018

Executive Summary/Highlights

A trade war with China. A fragile agreement with North Korea. A growing fear of Russian hackers. Ahead of the 2018 U.S. midterm congressional elections, geopolitical conflict continues to play out in cyberspace.

According to the world's top incident response (IR) professionals, politically motivated cyberattacks from nation-state actors have contributed to an ominous increase in destructive attacks: attacks that are tailored to specific targets, cause system outages and destroy data in ways designed to paralyze an organization's operations. Tom Kellermann, Carbon Black's Chief Cybersecurity Officer, put it this way: "These attackers aren't just committing simple burglary or even home invasion — they're arsonists."

Despite the heightened threat, most organizations still lack skilled security experts and don't have the visibility they need to challenge these ever-evolving cyberattacks. And with November's U.S. congressional elections fast approaching, at stake is not only significant financial loss, but also the trustworthiness of the country's political institutions.

To stay abreast of the current attack landscape and to quantify the latest attack trends seen by leading IR firms, Carbon Black publishes a Quarterly Incident Response Threat Report (QIRTR). **This is Carbon Black's second quarterly report** since introducing the QIRTR in July. This report aggregates qualitative and quantitative input from **37 Carbon Black IR partners**. The report's goal is to offer actionable intelligence for business and technology leaders, fueled by analysis of the newest threats, and expert insights on how to stop them.

Our research found that today's attackers are increasingly punitive, sophisticated and confident. And because of the dark web, they have access to complex tools and compromised infrastructures, including voter databases. This allows attackers to exploit new security vulnerabilities and operate at a higher level of sophistication than before.

"Our research found that today's attackers are increasingly punitive, sophisticated and confident."

— IR professional

Among the Key Findings

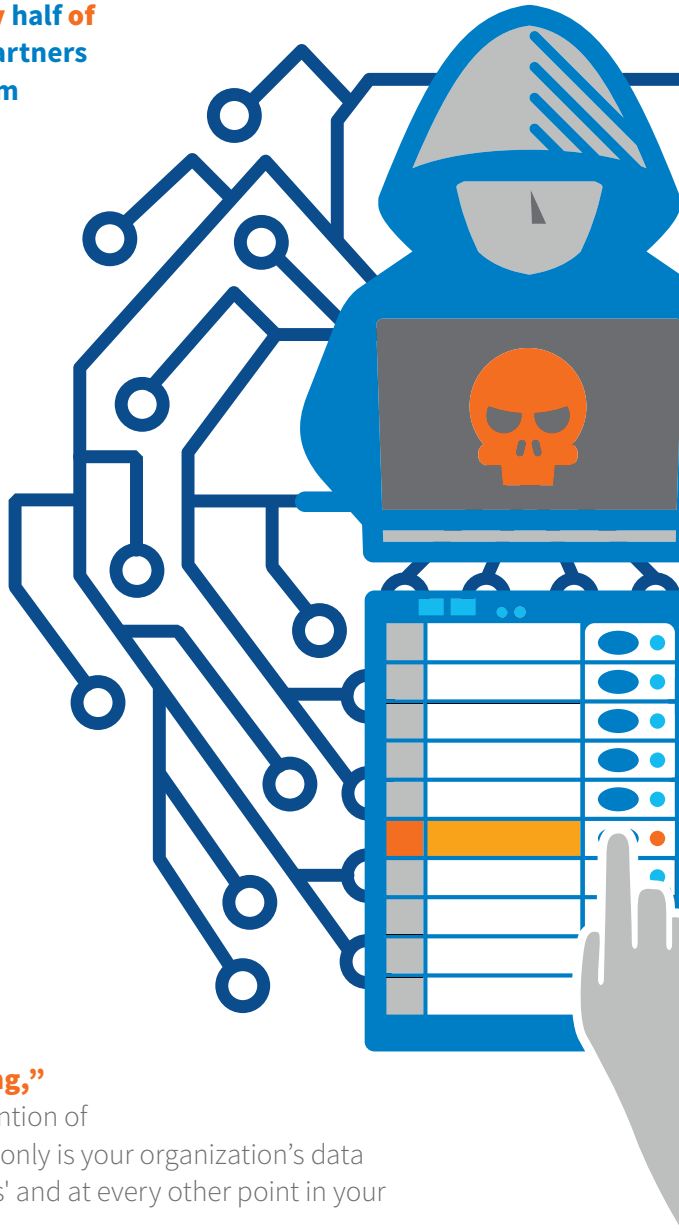
1. **China and Russia remain responsible for nearly half of all cyberattacks. Of 113 investigations our IR partners conducted in the third quarter, 47 stemmed from those two countries alone.** Iran, North Korea and Brazil were also the origin of a significant number of recent attacks.

2. **Destructive attacks are on the rise.** IR firms said that victims experienced **destructive attacks 32%** of the time.

3. **Two-thirds** of IR professionals believe **cyberattacks** will influence the upcoming U.S. elections.

4. **Compounding the threat to elections are marketplaces on the dark web**, a network of internet content not publicly accessible, offering several election-related items for sale, including voter databases, social media influence campaigns and hackers willing to conduct espionage campaigns.

5. **Over half of IR firms** encountered instances of **attempted counter incident response**.



6. **Half of today's attacks leverage "island hopping,"** whereby attackers target organizations with the intention of accessing an affiliate's network. This means that not only is your organization's data at risk, but so is the data at your customers', partners' and at every other point in your supply chain.

7. **A growing number of attacks are now taking advantage of Internet of Things (IoT) vulnerabilities** — and not just consumer devices. **An alarming 38%** of IR professionals saw **attacks on enterprise IoT devices**, which can be a point of entry to organizations' primary networks, allowing island hopping.

Politically Motivated Cyberattacks Threaten Democracy

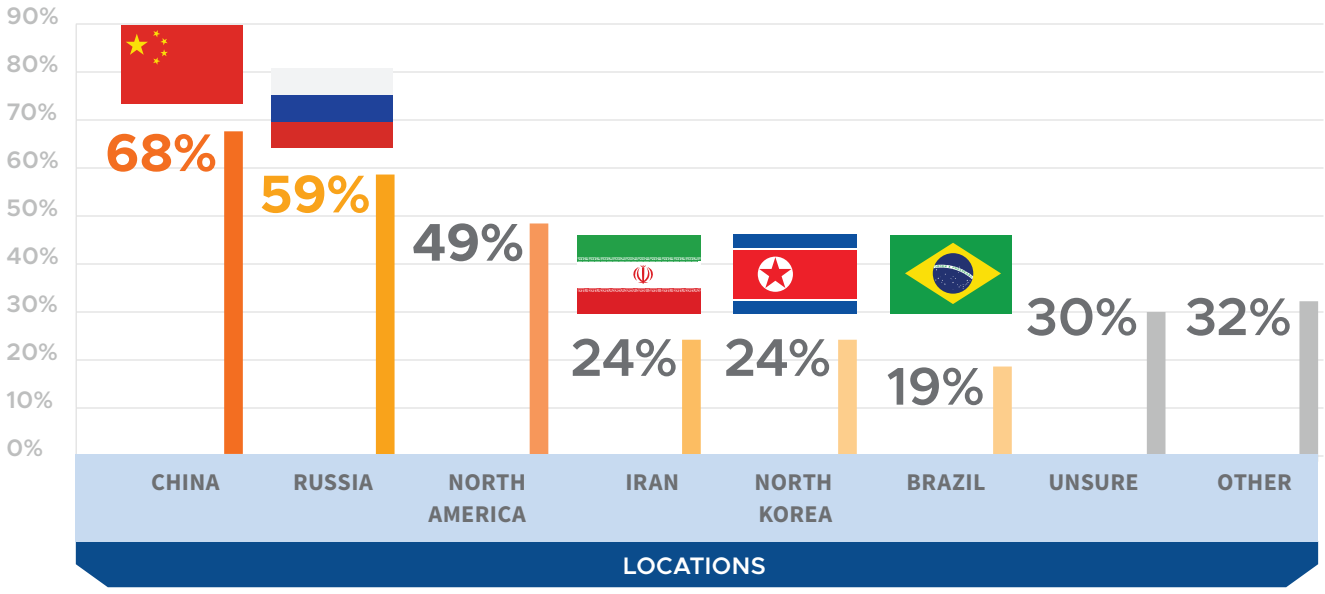
Whether it's for political manipulation or to gain an economic edge on their adversaries, nation-state actors in today's pressurized geopolitical landscape feel more emboldened and empowered than ever. It should come as no surprise that nearly half of all IR investigations conducted by IR firms stem from two countries: China and Russia. North Korea, Iran and Brazil were also the origin of a significant number of investigations.

Cyberattacks are becoming increasingly sophisticated, in large part because of a burgeoning dark web economy. Not only are complex tools becoming cheaper and more accessible, but the sale of compromised infrastructure can provide them a semblance of cover.

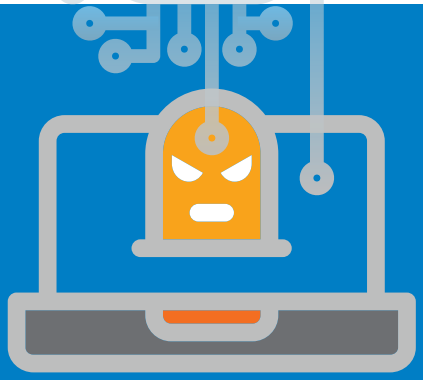
"More and more, state actors are using compromised infrastructures sold on the dark web as command and control outposts," one IR professional said. "Since these infrastructures are the site of a variety of other commodity activities, investigators will often block those actions and assume the case is closed. Meanwhile, the state actors remain behind running more covert operations."

FROM WHAT COUNTRIES ARE YOU SEEING CYBERATTACKS?

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



Carbon Black.



"More and more, state actors are using compromised infrastructures sold on the dark web as command and control outposts."

— IR professional

50%

CHINA AND RUSSIA REMAIN RESPONSIBLE FOR NEARLY HALF OF ALL IR INVESTIGATIONS.

Carbon Black.

The Dark Web & the 2018 Midterm Elections

Dark web markets and freelance websites offer a selection of resources for those wishing to conduct nefarious activities specifically relating to the 2018 midterm elections. In conducting its research, Carbon Black found several interesting dark web offerings:

1. **VOTER DATABASES FOR SALE —** Carbon Black researchers found 20 different state voter databases available for purchase on the dark web, several from swing states. Critical information in these offerings included voter IDs, full names, current / previous addresses, genders, phone numbers and citizenship status, among other information. Entities wishing to influence voters can use this type of information to send targeted election-related campaign materials to their desired audience, among other influential activities.

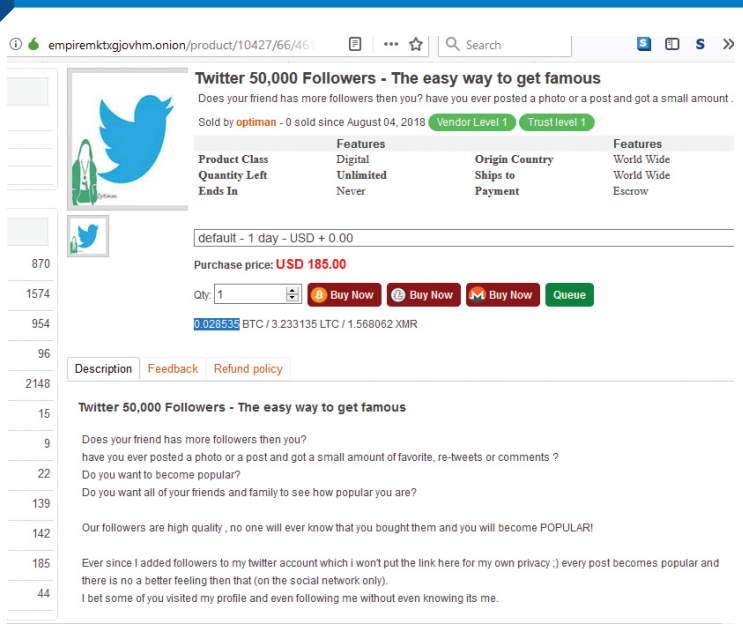
VOTER DATABASES FOR SALE

STATE	NUMBER OF VOTER RECORDS FOR SALE
Alabama	132,788 voters
Alaska	487,415 voters
Arkansas	1,700,000 voters
Colorado	3,500,000 voters
Connecticut	2,300,000 voters
Delaware	645,327 voters
Florida	12,500,000 voters
Georgia	6,600,600 voters
Michigan	7,400,000 voters
Nevada	1,160,000 voters
New Jersey	5,500,500 voters
New York	15,000,000 voters
North Carolina	7,400,000 voters
Ohio	7,900,000 voters
Oklahoma	2,158,410 voters
Pennsylvania	620,201 voters
Rhode Island	740,049 voters
Texas	657,695 voters
Utah	731,639 voters
Washington	4,400,000 voters
TOTAL	**81,534,624 VOTERS**

Carbon Black.

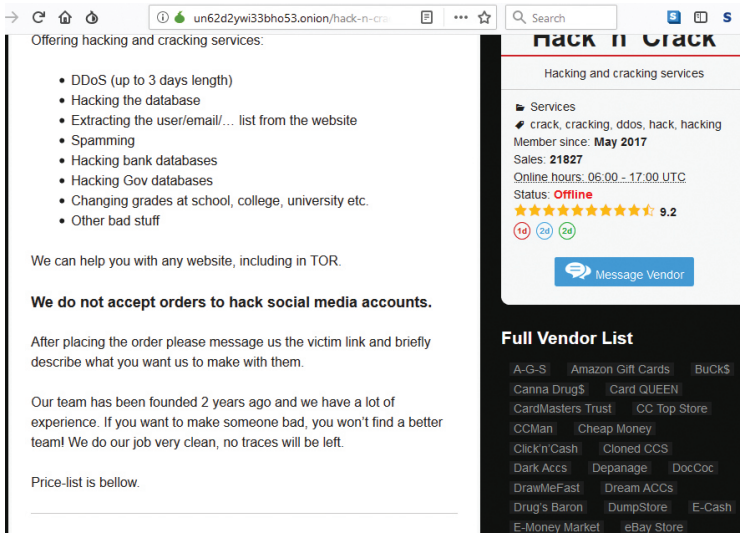
2.

HACKING/MANIPULATING OF SOCIAL MEDIA SITES — Thousands of Instagram followers, Facebook likes, YouTube views and Twitter retweets are available for a small amount of cryptocurrency on the dark web. Some listings focus on selling "laser-focused" ads to make sure a message gets across to the recipients — most likely to respond to a campaign. Manipulating social media is a relatively low-cost endeavor, and hackers on the dark web appear to have tools at the ready for manipulating public opinion on major American platforms.



3.

HACKERS FOR HIRE — Freelance hackers and hacking teams have a significant underground presence and it's easier to find these groups now that there are search engines created specifically for the dark web. Some of these hackers offer to target government entities for the purposes of database manipulation, economic/corporate espionage, DDoS attacks and botnet rentals. These custom services cost hundreds to thousands of dollars per target, unlike many generic hacks offered on dark web marketplaces.



Election-focused cyberattacks now pose real threats to Western political institutions. **Sixty-eight percent of survey respondents**, among the top cybersecurity professionals in the world, believe the upcoming U.S. midterm elections will be influenced by cyberattacks. According to a Carbon Black survey gauging voter confidence, one in four voters said the fears of such attacks would make them reconsider voting. As a result, as many as 58.8 million people might simply stay home on Election Day because of cybersecurity fears.

For nation-state actors, it's not just about directly targeting, say, voting machines — though that is certainly one viable option. Rather, attackers are looking to political propaganda operations, such as Russia's 2016 hack of the Democratic National Committee. As one IR professional explains, "They're doing hack and leak campaigns, targeting media providers, political parties, voter databases, they're using social media…all to build narratives that disenfranchise potential voters and damage the reputations of democracy without having to do direct interactions, which can be riskier."

Politically motivated cyberattacks are, of course, nothing new — one IR professional suggests they've been going on for at least the past five or six election cycles. But they used to be limited in scope and used mostly for political intelligence. "What's new — and dangerous," the IR professional says, "is the propaganda element."

"They're doing hack and leak campaigns, targeting media providers, political parties, voter databases, they're using social media…all to build narratives that disenfranchise potential voters and damage the reputations of democracy without having to do direct interactions, which can be riskier."

— IR professional

An Ominous Rise in Destructive Attacks

As nation-state cyberattackers become more sophisticated and powerful, their attacks become increasingly destructive — **our respondents said victims experienced such attacks 32% of the time**.

One IR professional recounts firsthand experience: "We've seen a lot of destructive actions from Iran and North Korea lately, where they've effectively wiped machines they suspect of being forensically analyzed."

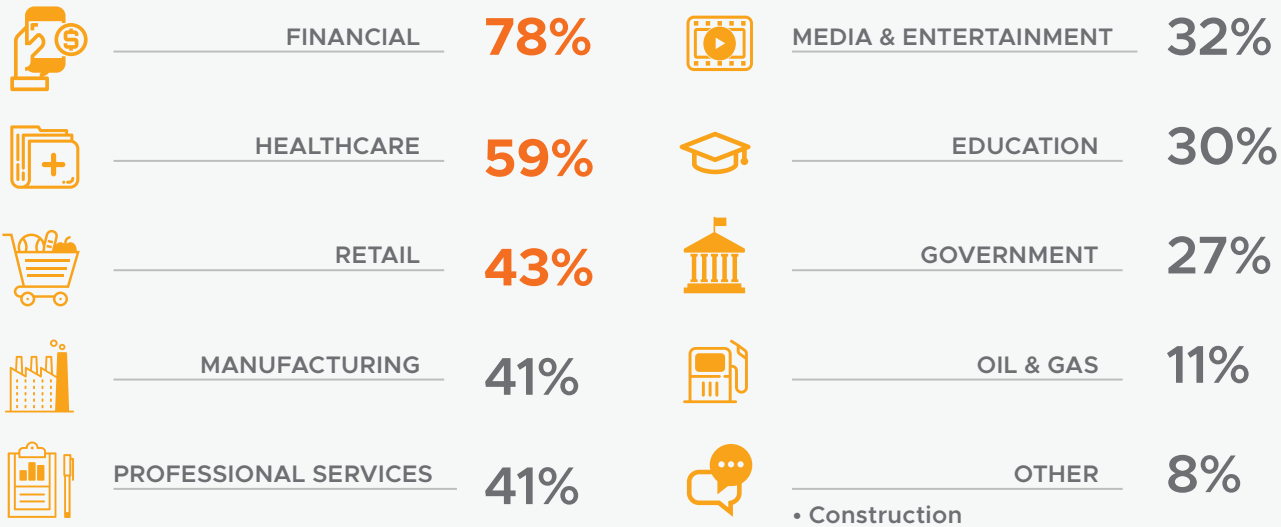
And as one might expect, these attacks are industry agnostic, impacting a wide range of different verticals. **Financial and healthcare organizations remain the most targeted (78 and 59 percent of respondents saw those industries targeted by cyberattacks**, respectively), followed by **retail (43%)**, **manufacturing (41%)**, and **government (27%)**.

The targeting of manufacturing businesses grew steeply from last quarter — which, according to one IR professional, "would seem unusual, given that it's not a liquid sector — it means that these attacks are purely punitive or attempts to manifest a physical event."

Another IR professional added, "With instances of espionage, we've seen attackers leverage their highest end capabilities to go after industrial bases and tech service providers — especially those high-tech researchers on aerospace, power generation, oil and gas, and nuclear."

WHAT VERTICALS ARE YOU SEEING TARGETED BY CYBERATTACKS?

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



Carbon Black.

The rise in destructive attacks should be even more worrisome for organizations given that **50% of all attacks now leverage island hopping** — which means a vulnerability puts not only your organization at risk, but those of your customers and partners as well. In the third quarter, **30% of respondents also saw victims' websites converted into a watering hole**, another type of attack where attackers use a company's network as a means of attacking an associated company within a network.

But how to explain the growing severity of cyberattacks in 2018?

As previously discussed, geopolitical tensions play a significant role. "Hackers are acting as cyber militias," Kellermann noted. "They're paying homage to their regime, and, as such, their reactions to foreign attempts to stop them will be punitive in nature."

The situation has been exacerbated by the fact that the cybersecurity community in the West is simply getting better at IR. "Attackers want to cover their tracks because they're feeling the pressure from law enforcement," one IR professional says.

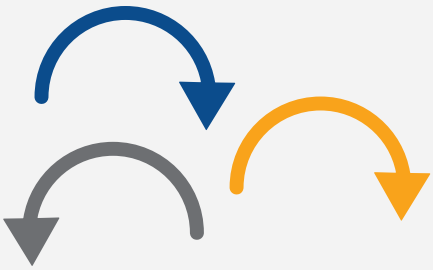
But there's also a psychological element at play. The dark web respects force, and strength is demonstrated by taking destructive measures. And who's to stop them? After all, **only approximately 5% of all cyberattacks are prosecuted**. This has led, especially among younger attackers, to something of a "demigod complex."

The U.S. has responded to a lack of prosecution with a "naming and shaming" policy for cyberattackers. Such tactics can prove counterproductive.

"It suits them to be blamed," one IR professional observed of Russian hackers. "Getting publicly outed fits into their government's narrative of them being victims of the West."

It's also a matter of having better access to tools — tools that enable attackers to cover their tracks and customize their operations to a target. Some Chinese cybercriminals, for instance, have moved away from their "once predictable tool set" and begun to "beg, borrow and steal from other operators," said another IR professional. They can be more flexible because the Chinese government, to claim plausible deniability, has subcontracted these operations out to shell companies — purposefully blurring the lines between nation-state activity and that of organized crime. "It's much easier for them to cross lines into data destruction when they're not technically directly accountable to their government," he added.

50% OF IR FIRMS HAVE ENCOUNTERED AN ATTACK LEVERAGING **ISLAND HOPPING**



Carbon Black.

CASE STUDY: A Sophisticated Revenge Plot, Foiled by IR

It's a company's worst nightmare: While performing routine maintenance activities, the Information Technology department finds that a newly acquired company has been locked out of up to 50 virtual private network (VPN) devices, which govern primary and backup access to roughly 30 branch locations. Then it gets worse — the central Amazon Web Services (AWS)-hosted virtual router is down, and when it's powered back on, they find the VPN configuration files and routing tables have been deleted from the server, as well as 14 days' worth of backups.

A wide-scale network outage ensues. Revenue loss starts to add up. The attack impacts not only the newly acquired company, but the parent company too, as the attackers "island hop" from one network to the other. Fortunately, two potential suspects are quickly identified: employees of the newly acquired company disgruntled with their new roles (who had expressed as much in several vulgar email exchanges).

Upon being brought in, Nisos' first move was to deploy Carbon Black to gain visibility across all of the newly acquired company's endpoints. Carbon Black allowed them to identify several hosts with Hide Tools on them (a commercially available technology that monitors and tracks users) and, subsequently, the system that appeared to have installed the tool. Nisos decided to observe the suspected attackers' activities using Talon — a Nisos platform that integrates with Cb Live Response to track data on and off the network.

By tagging documents on the network, Nisos was able to track data exfiltration beyond managed network assets (where Carbon Black was installed), which helped them determine the nature and source of the attack to hosts that were not covered under the Carbon Black deployment. Namely, they found files opened from a virtual private server (VPS) that, at one time, hosted the company's old website but was no longer under positive control of the network security team. The former employees still had access to the VPS and were using it to launch attacks onto the network. At the same time, they attempted to liquidate the overages in the VPS provider account, which they had intentionally overpaid — to the tune of nearly $20,000.

Despite counter incident response maneuvers — encrypting data, source code and other information; wiping batch history and deleting logs — Nisos, using Carbon Black and Talon, found and examined private chat logs, communications and AWS cloud logs that implicated the two former employees. They quickly remediated the issue and referred the case to law enforcement for prosecution.

Counter Incident Response, Destruction of Logs, Lateral Movement & Secondary C2 on a Sleep Cycle

As cyberattackers gain more access to complex tools and launch more sophisticated attacks, they find new network vulnerabilities and new ways to exploit network architectures.

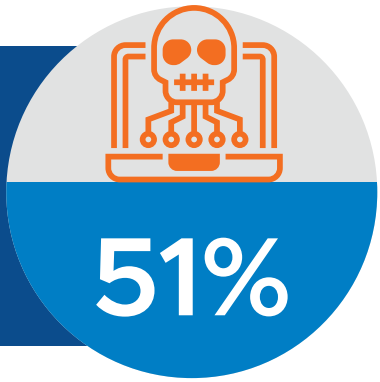
Attackers' growing sophistication is evident in the rising instances of counter incident response, which occurred in **over half (51%) of all incidents** seen by respondents in the last 90 days.

It's fitting, given the destructive nature of contemporary attacks, that **72%** of IR professionals saw counter IR in the form of **destruction of logs**. One IR professional recounts: "We've seen a lot of destruction of log data, very meticulous cleanup of antivirus logs, security logs and denying IR teams the access to data they need to investigate." In other instances, the IR professional said attackers are also stealing network architecture diagrams to find routes in and out of an organization.

In the third quarter, **an alarming 41% of respondents encountered instances where networkbased protections were circumvented**. Respondents reported observing secondary C2 used on a sleep cycle — suggesting that network-based protections

51% OF IR PROFESSIONALS SEE
COUNTER INCIDENT RESPONSE DURING IR ENGAGEMENTS

Carbon Black.



"We've seen a lot of destruction of log data, very meticulous cleanup of antivirus logs, security logs and denying IR teams the access to data they need to investigate."

— IR professional

which are regularly deployed to shut off hackers' secret passages in your network (C2), have ostensibly been rendered useless; attackers are using a second C2 that wakes up only after the initial one goes down.

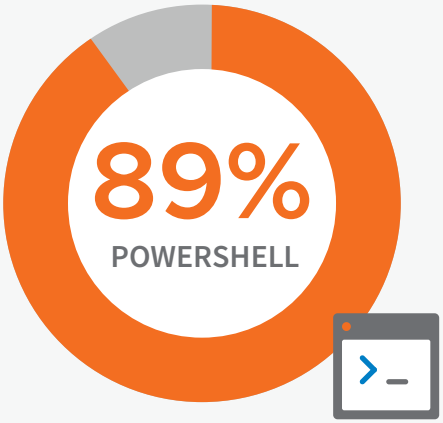
Attackers are also finding new ways to facilitate lateral movement within networks. While the exploitation of **PowerShell** and **WMI** are to be expected, the prominence of using **malicious script hosts (35%)** and legitimate OS application tampering via **process hollowing (38%)** represent, as one IR professional says, "a heightened tenacity and sophistication among attackers" — as both represent rather complex techniques.

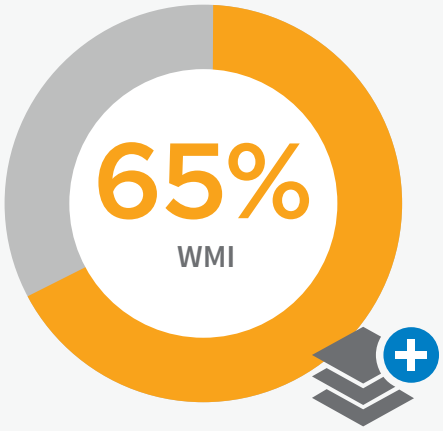
Some nation-state actors like China are even finding ways to infiltrate and move around a network using the native tool set of the organization. "It's low-observable," said one IR professional. "It allows them to get in for espionage purposes and collect information."

At the same time, the move to cloud service products like Dropbox opens new vulnerabilities, both in the products themselves and IT teams' knowledge of them. In fact, when asked about the top barrier to incident response, 27% percent of respondents chose a shortage of skilled security experts. One IR professional suggests that, when it comes to cloud services, "People trick themselves into thinking they know how to work these products, but don't realize that you can easily move things onto the cloud and leave buckets open for the world to see."

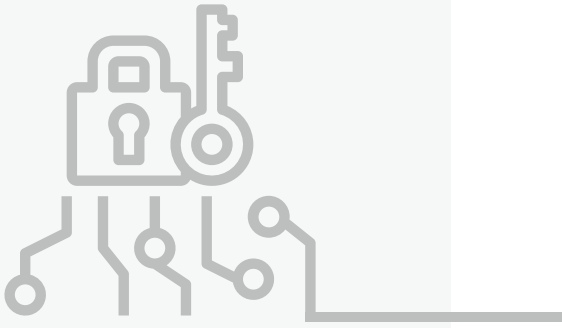
Another IR professional has seen a rise in phishing attacks on various cloud service product suites. "No matter how many times employees are trained not to respond to these phishing attempts, a small percentage will persistently get through."

WHICH DUAL-PURPOSE TOOLS FACILITATE LATERAL MOVEMENT FOR ATTACKERS MOST?





Carbon Black.



A Growing Concern: Internet of Things (IoT)

38% OF IR FIRMS SAID THEY SAW ATTACKS AGAINST **ENTERPRISE IoT DEVICES**

Today, there are more than **8.4 billion IoT devices**, ranging from consumer devices like Fitbits and smart watches to enterprise devices such as security cameras, alarm systems and thermostats. Of late, those "things" — which often have no built-in ability to be patched remotely — have become the target of cyberattacks. In 2016, for instance, a Russian botnet called Mirai gained access to a veritable army of closed-circuit TV cameras, which led to a denial of service attack that left huge swaths of the internet inaccessible to many on the East Coast of the U.S.

In a new addition to our report, we asked IR firms about incidents they've seen wherein attackers take advantage of IoT-related vulnerabilities. **Fifty-four percent** of IR firms said they saw attacks on **consumer devices**, but a worrisome **38%** said they saw attacks on **enterprise devices**. Compromised IoT devices are of concern because they can be used to "island hop" onto an organization's primary network. "It's a meaningful segmentation of a network," says one IR professional. "Which means they're fairly susceptible to island hopping. Protecting IoT requires the ability to protect each endpoint across your organization."

"The increasingly destructive nature of cyberattacks reflect an environment rife with geopolitical tension."

— **Tom Kellermann, Carbon Black Chief Cybersecurity Officer**

Conclusion

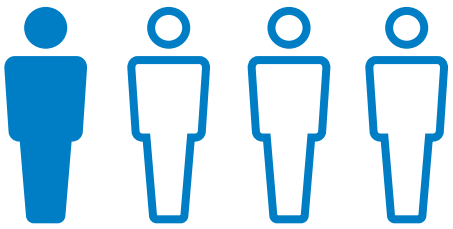
The increasingly destructive nature of cyberattacks reflect an environment rife with geopolitical tension — one where attackers, empowered by their access to the most complex of tools, exploit new vulnerabilities and employ sophisticated counter incident response techniques. That IR has gotten better — but has not led to more prosecutions — only emboldens these attackers more.

Organizations who remain unprepared risk not only their own financial loss, but those of their customers and partners as well. But with the U.S. midterm elections fast approaching, the risks are more than financial in nature — the rise in cyber campaigns aimed at undermining democratic institutions pose graver threats than ever before.

The top barrier to effective IR remains a lack of visibility. IR professionals can't hunt down threats if they can't see into all aspects of an enterprise's network, which now includes a growing number of at-risk endpoints produced by IoT devices and cloud services.

These attacks won't slow down. But if we can see them better — through heightened visibility across networks — and quickly detect attacks, we can surely do a better job of stopping them in their tracks.

1 in 4 VOTERS SAID THEY WILL CONSIDER NOT VOTING IN FUTURE ELECTIONS OVER CYBERSECURITY FEARS



= **58.8 MILLION PEOPLE**

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including approximately one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.

Politically motivated cyberattacks are, of course, nothing new — one IR professional suggests they've been going on for at least the past five or six election cycles. But they used to be limited in scope and used mostly for political intelligence. "What's new — and dangerous," the IR professional says, "is the propaganda element."

Carbon Black.

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

carbonblack.com