



# One Year Out From the 2020 U.S. Elections, Geopolitical Tension Continues to Spawn Cyberattacks

NOVEMBER 2019



## Executive Summary

Geopolitical tension is, once again, playing out in cyberspace.

According to VMware Carbon Black's latest Global Incident Response Threat Report (GIRTR), top incident response (IR) professionals around the world say ongoing geopolitical tensions involving China, Russia, North Korea and Iran are leading to cyberattacks.

"The axis of evil in cyberspace is alive and well," said Tom Kellermann, VMware Carbon Black's head cybersecurity strategist.

According to VMware Carbon Black's latest research, **the majority of today's cyberattacks now include tactics such as lateral movement, island hopping and destructive attacks.** Advanced hacking capabilities and services for sale on the dark web compound the issue, as does an unprecedented collaboration among nation-states. These

realities pose a tremendous risk to targets with decentralized systems protecting high-value assets, including money, intellectual property and state secrets.

Targets who fail to increase their defenses accordingly are paying an ever-steeper price, as the frequency of destructive attacks continues to climb, according to the research. Financial gain drove most attacks in 2019, the research found, but IR professionals said they are also concerned about these same tools being deployed to interfere with the U.S. elections in 2020.

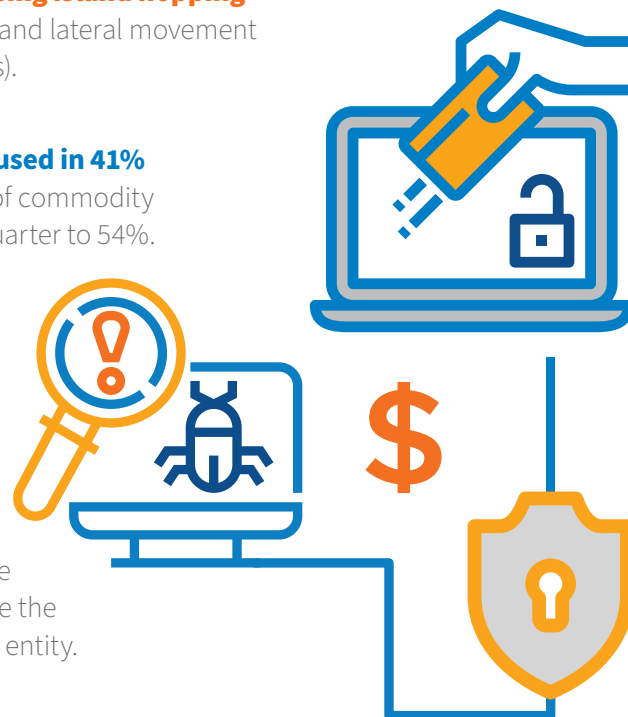
This is the fourth edition of VMware Carbon Black's semiannual Global Incident Response Threat Report, tracking the latest attack trends seen by leading IR firms. The report aggregates qualitative and quantitative input from 30 VMware Carbon Black IR partners for the latest edition.



As cooperation among attackers increases, this report highlights the efforts of VMware Carbon Black and its IR partners to fight back as a global community with actionable intelligence and holistic strategies to mitigate the ongoing cyber insurgency online.

## Key Research Highlights:

- 1** **China and Russia are responsible for the lion's share of cyberattacks in 2019.** When asked which country accounted for the most attacks, IR professionals said **Russia (29%) and then China (18%)**, followed by North America (11%) and North Korea (4%).
- 2** **Financial gain was the primary motivation for 90% of attacks, a sharp increase from 61% in the first half of 2019** and a shift from previous years, when intellectual property theft and stealing customer information topped the list.
- 3** **IR pros said they experienced destructive/integrity attacks in about 41% of attacks, a 10% increase on the past two quarters.** This is an ominous trend as cyberspace is becoming more punitive.
- 4** **There has been a continued rise in attackers using island hopping (41% of total attacks, up 5% since Q1 of 2019)** and lateral movement (steady at 67% of attacks, well above 2018 averages).
- 5** **Attackers are adapting. Custom malware was used in 41% of attacks, up from 33% in Q1 of 2019.** The use of commodity malware has seen a slight decline, from 57% last quarter to 54%.
- 6** **There's been a significant increase in use of outside threat intelligence feeds – 57% this quarter** compared to 14% last quarter.
- 7** **Among respondents working in the U.S., 59% said risk around election process and security has increased** to a significant extent since 2016. Within that same group, **65%** said they believe the 2020 U.S. elections will be influenced by an outside entity.
- 8** **Voter databases from previous elections are readily available from high-reputation vendors on the dark web for less than \$100.** In total, from a single listing, information on more than 81 million voters is currently available for sale.



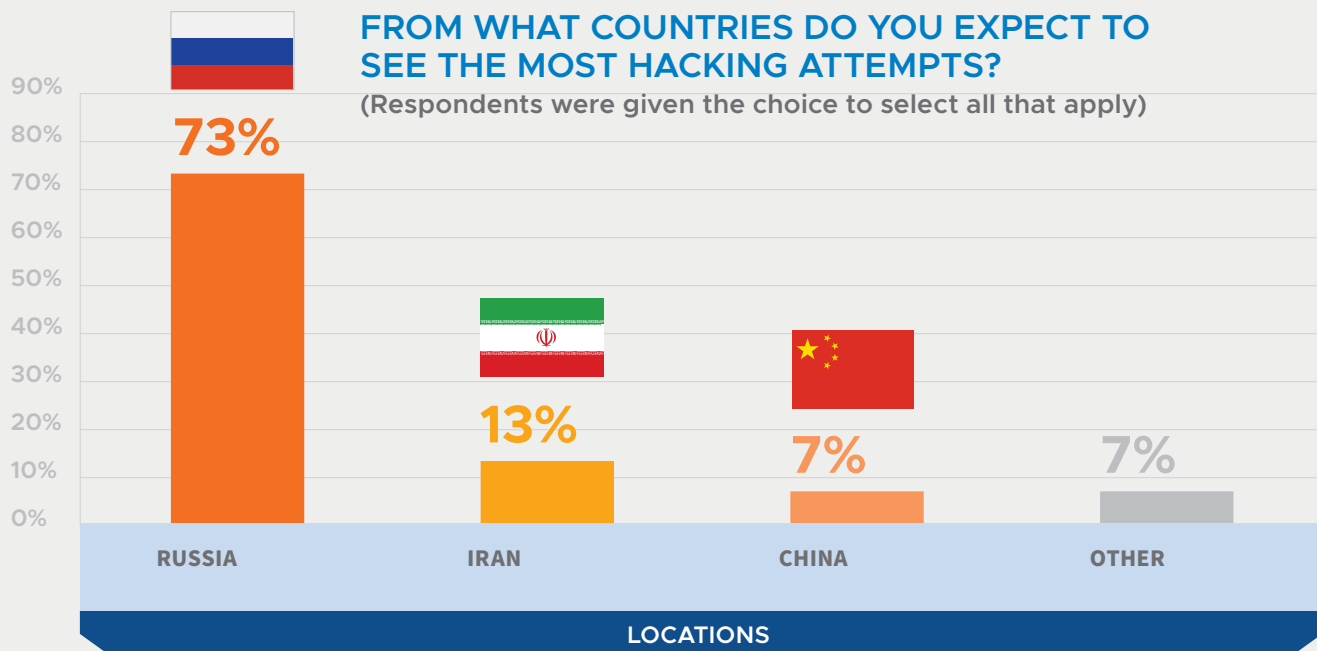
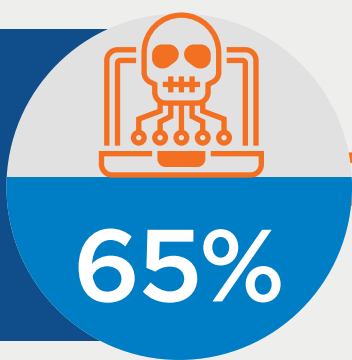
# One Year Away From the 2020 U.S. Elections

Almost two-thirds of IR professionals believe the 2020 U.S. elections will be influenced by a cyberattack from an outside entity, according to our research. Russia is viewed as the most likely

source of such attacks, at 73%, followed by Iran at 13% and China at 7%. This underscores a point made by FBI Director Christopher Wray during a congressional hearing in October:

65% OF IR PROFESSIONALS BELIEVE THE 2020 PRESIDENTIAL ELECTION WILL BE INFLUENCED BY A CYBERATTACK

vmware Carbon Black



**“All of those countries in different ways are clearly interested in engaging in malign foreign influence,”** Wray said of Iran, North Korea and China. As for Russia, he said, the U.S. expects that they **“already have continued to up their game from what they did in 2016.”**

Echoing Wray’s insights, 59% of IR professionals said risk about our election process and security has increased a significant extent since 2016. Almost 95% of respondents said they are most concerned about the spread of misinformation/ disinformation relating to the integrity of the 2020 elections. The threat isn’t only emanating from countries that want to see the current administration reelected, as China and Russia have divergent geopolitical goals.

Voting machines, voter rolls and state election websites are perceived to be at risk of interference, according to our survey. It’s worth remembering that Russia targeted election systems in all 50 states in 2016, though there is no evidence it changed vote tallies.



## THERE ARE THREE WAYS ATTACKERS CAN UP THEIR GAME IN 2020

1

### VOTER ROLL MANIPULATION

Voter registration systems and databases are managed on a state-to-state basis and are often built on unsecure technology. Attackers may try to manipulate results in swing states or alter the integrity of voter records for a particular party, changing names or addresses to prevent people from voting.

2

### STATE WEBSITE DEFAACEMENT

Most states manage websites that show real-time results on Election Day, which then informs the local media coverage. These systems can be easily manipulated by attackers to show false values, creating confusion and distrust among the voting populace, potentially keeping some groups away from the polls.

3

### MEDIA ISLAND HOPPING



Major media outlets, particularly those with a strong partisan stance, may be targeted and their social channels may be manipulated. This could take the form of sockpuppet accounts that spread disinformation, or data mining of these channels’ followers for potential target lists.



**The tools to conduct these influence campaigns and attacks on election infrastructure are available in a thriving market on the dark web, VMware Carbon Black researchers have found.**

**Voter Databases for Sale:** Current listings for state voter database dumps are currently available for sale on the dark web. One vendor even offers bundles that include combined voter databases from 27 states, rather than offering each state individually. One such bundle has been sold for roughly \$95 at least 47 times as of last October. This suggests that the raw data in each database dump — which might include names, addresses, birthdays, genders, phone numbers and citizenship information — continues to be useful in a variety of ways. In total, from a single listing, information on more than 81 million voters is available. For context, approximately 250 million people voted in the 2016 presidential election in the U.S.

**USA Voter Database Pack (27 States)**

**Seller Level 0 (47)**  
**Trust Level 1 (9K)**  
**Verified Seller: 2 / Trusted**  
**Seller: 2**  
**Positive Feedback: (100%)**  
**Member since: May 22, 2019**  
**Last Login: Oct 16, 2019**  
**Sales: 47**  
**Orders: 0**  
**Disputes: 0**

**Member Type: Seller**  
**Origin Country: World Wide**  
**Ship To: World Wide**  
**Payment: Escrow**  
**Product class: Digital Goods**  
**Quantity: (1 Auto Dispatch Items)**  
**Unlimited Available**

**Sale Price: 90.60 EUR / 0.01227377 BTC**  
**Sale Price: 90.60 EUR / 1.84075847 XMR**  
**Sale Price: 90.60 EUR / 1.81733916 LTC**  
**Sale Price: 90.60 EUR / 0.44806417 BCH**


## 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**

**Social Media Influence:** Dark web marketplaces continue to show listings for bots to hack social media sites, but there are fewer listings available than in previous iterations of this research — likely the result of additional security measures introduced by social media companies. Bots are currently available for about \$12 to create large numbers of followers or accounts across multiple platforms at the same time, improving the likelihood that content begins to go viral.

Huge Bot Pack (Google, Facebook, Youtube, Twitter)




**Seller Level 2 (495)**  
**Trust Level 1 (9K)**  
 Verified Seller: 2 / Trusted  
 Seller: 2  
 Positive Feedback: (83%)  
 Member since: May 11, 2019  
 Last Login: Oct 16, 2019  
 Sales: 495  
 Orders: 0  
 Disputes: 0

Member Type: Seller  
 Origin Country: World Wide  
 Ship To: World Wide  
 Payment: Escrow  
 Product class: Digital Goods  
 Quantity: (1 Auto Dispatch Items)  
 Unlimited Available

Sale Price: 0.90 EUR / 0.00012152 BTC  
 Sale Price: 0.90 EUR / 0.01822533 XMR  
 Sale Price: 0.90 EUR / 0.01799346 LTC

Huge Bot Pack (Google, Facebook, Youtube, Twitter) And More!



**Seller Level 1 (92)**  
**Trust Level 1 (9K)**  
 Verified Seller: 2 / Trusted  
 Seller: 2  
 Positive Feedback: (100%)  
 Member since: Mar 30, 2018  
 Last Login: Oct 16, 2019  
 Sales: 92  
 Orders: 7  
 Disputes: 0

Member Type: Seller  
 Origin Country: Portugal  
 Ship To: World Wide  
 Payment: Escrow  
 Product class: Digital Goods  
 Quantity: Unlimited Available

Sale Price: 5.99 EUR / 0.00081151 BTC  
 Sale Price: 5.99 EUR / 0.12217010 XMR  
 Sale Price: 5.99 EUR / 0.12018459 LTC

**Negative SEO Attacks:** Attackers continue to offer their services to customers for between \$200 and \$500 or more, usually for specific jobs such as hacking a social media account or web servers or performing DDoS attacks. One new approach is the negative SEO (search engine optimization) attack, which usually costs about \$150 and attempts to manipulate search engines to return results that could be damaging to a candidate.

About

contact> wickr [redacted] for any help more especially for your orders as we order top quality products and we have a long reputable and remarkable service as we do 100% discreet packaging which goes through customs, all we need is long term business relationship so we urge you to try our service as you will have no regret thanks.

Purchase

Type: Mail Shipping from: United States Country: Worldwide

Package name Price

1 200 USD

About

Clean your criminal records Recover stolen bitcoins from scammers Fix your credit history and score Grades Change Cell phones Hacking Emails Hacking Social Media Hacking Malicious Software Website Hacking PC Hacking DDoS Skype Hacking IP Tracking Debt clearing Social Engineering Reverse Engineering Server Hacking Web Server Hacking Buffer Overflows Wireless Hacking Password Cracking Malware/Ransomware .Gmail [redacted] wickr [redacted] whatsapp [redacted]

Purchase

Type: Mail Shipping from: United States Country: Worldwide

Package name Price

NEGATIVE SEO ATTACK: SINK YOUR COMPETITORS WEB RANKING (WITH PROOFS)



**Seller Level 0 (10)**  
**Trust Level 0 (0K)**  
 Verified Seller: 0 / Trusted  
 Seller: 0  
 Positive Feedback: (0%)  
 Member since: Oct 13, 2019  
 Last Login: Oct 18, 2019  
 Sales: 0  
 Orders: 0  
 Disputes: 0

Member Type: Seller  
 Origin Country: World Wide  
 Ship To: World Wide  
 Payment: Escrow  
 Product class: Digital Goods  
 Quantity: Unlimited Available

Sale Price: 134.14 EUR / 0.01862447 BTC  
 Sale Price: 134.14 EUR / 2.74977055 XMR  
 Sale Price: 134.14 EUR / 2.79017857 LTC

WHAT WILL I DO?

I will send thousands of trash unnatural backlinks to your competitor that will result in a heavy drop in Google results when unnatural link growth is detected. The links are sent from shady sources.

Recover a negative SEO attack is extremely hard and require lot of effort in creating new natural links and contents. It will take months to fix the issues of attack. Eventually, maybe your competitor have to close everything because of all technical implications of this attack and the difficulty to recover Google ranks.

## Best Practices for Protecting Critical Infrastructure Enterprises



**1 Baselining Vulnerabilities:** It is critical to get a baseline for where vulnerabilities lie, which can be done through a baseline “red team” or “purple team” audit and/or cyber hunt exercise. Penetration tests and general audits are also recommended.



**2 Multi-Factor Authentication:** MFA with just-in-time administration should be deployed to web servers holding key data. Websites accessible to the general public should be continuously reviewed for accuracy.



**3 Application Control:** Deploying application control helps protect critical servers by ensuring servers do not unnecessarily access the internet and blocking all unauthorized files or memory modifications.



**4 Micro-Segmentation:** Flat networks are more susceptible to hacking methods like lateral movement. Micro-segmentation divides the data center into distinct security segments, which are then assigned unique controls and services.



**5 Big Data:** Visibility is key when you’re under attack, and leveraging data and analytics is crucial to creating a window into what’s happening, or what happened.



**6 Integration:** Integrating critical security systems across your network (endpoints, firewalls, SIEMs, etc.) can allow automation that alleviates staffing and resource burdens.



**7 Threat Hunting:** Standing up threat hunting teams puts your organization in an active position, rather than reactive, and provides insight that goes well beyond simply responding to alerts.



**8 Collaboration:** Staying up to date on the latest attack methodologies, as well as attack vehicles — by sharing data and intelligence with a trusted user community — is a critical component to a strong security posture.



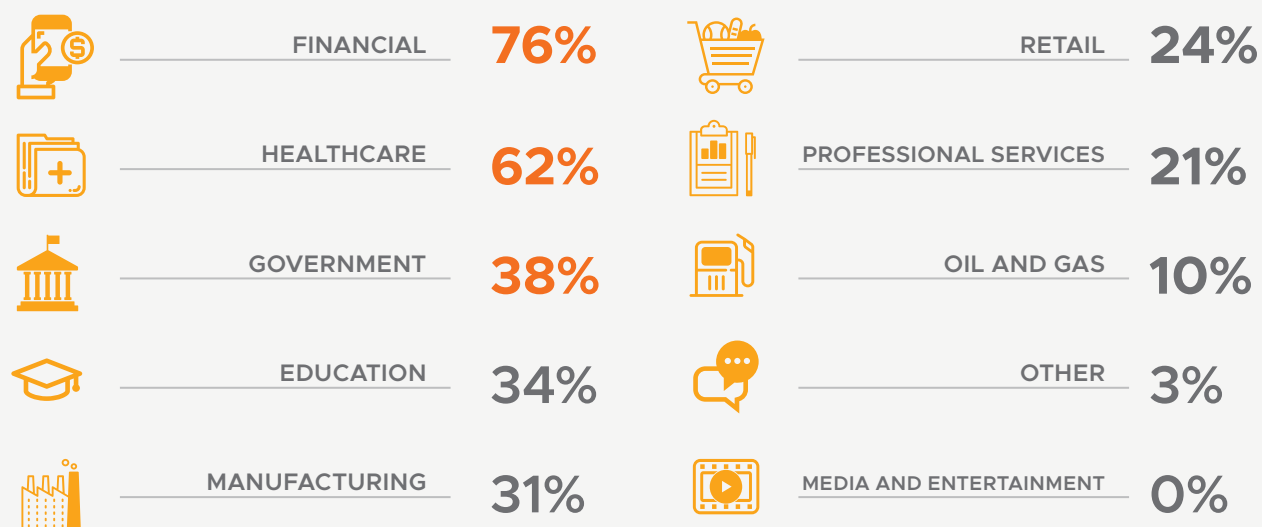
## Cyberattack Evolution

We're in the age of the modern bank heist. Our latest survey of IR firms supports VMware Carbon Black research showing that the financial sector is increasingly under threat from attackers using tools and methods that easily skirt traditional defenses and often avoid detection for weeks or months once they're in.

More than three-quarters of respondents said the financial industry is most often targeted by attacks, followed by healthcare, government and education.

### WHAT VERTICALS ARE YOU SEEING TARGETED BY CYBERATTACKS?

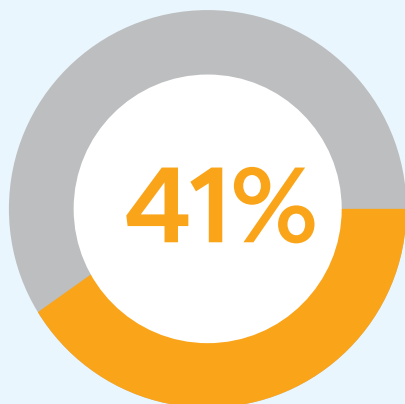
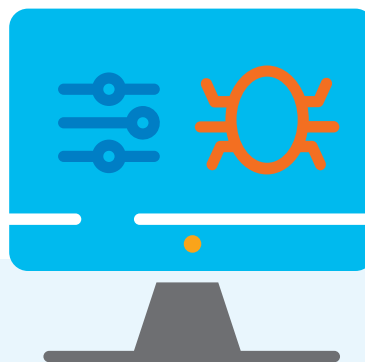
(Percentages added may exceed 100 since participants could select more than one answer for this question)



This mirrored the findings in VMware Carbon Black's Modern Bank Heists report in March, which found that 67% of surveyed financial institutions reported an increase in cyberattacks in the previous 12 months. Additionally, 79% of surveyed financial institutions said cybercriminals have become more sophisticated.

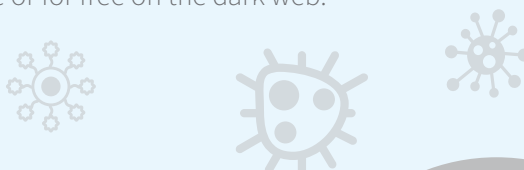
The use of more sophisticated and destructive methods during attacks has only increased in the months since. Two of the major new developments that cybersecurity firms have seen in 2019 are increases in custom malware and process hollowing.

“It really highlights the arms bazaar of the dark web and speaks to the fact that there is a true economy of scale, that there’s professional services being offered — much like consulting firms — to develop custom malware,” said Kellermann.



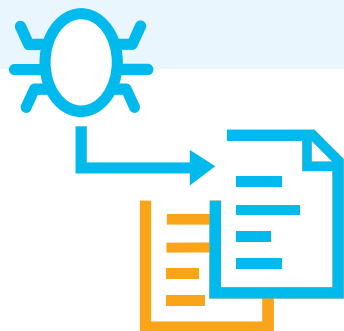
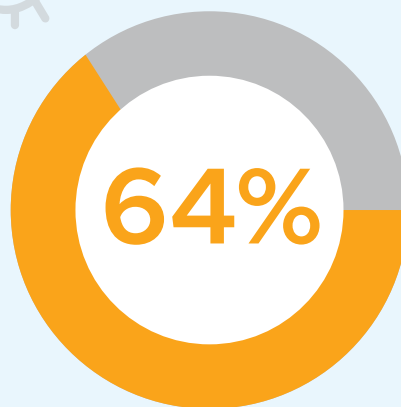
### CUSTOM MALWARE WAS USED IN 41% OF ATTACKS, UP FROM 33% IN Q1 OF 2019.

**Definition:** Custom malware is coded with a specific purpose in mind, a sign of more sophisticated and well-financed attacks, as opposed to commodity malware, which is widely available for purchase or for free on the dark web.



### PROCESS HOLLOWING HELPED FACILITATE LATERAL MOVEMENT FOR ATTACKERS 64% OF THE TIME, UP 8% ON LAST QUARTER AND 26% ON Q4 2018.

**Definition:** Process hollowing tricks operating systems and monitoring tools into thinking a legitimate process is running, when in fact the process’s memory has been hollowed out and replaced by a second, malicious program.



Greg Foss, senior threat researcher at VMware Carbon Black, said protecting against process hollowing requires endpoint detection and response tools. “It gives you that visibility into the parent process, the child process and what kicked off that whole chain of events.”

## Island Hopping

Cybercriminals are expanding their use of island hopping to creep into systems at their most vulnerable points, then hopping to higher-security parts of the network.

More than forty percent of attacks targeted victims through island hopping, up 5% from Q1 2019 and continuing a trend we've been seeing for the past two years.

VMware Carbon Black research has also found that attackers are selling island hopping access to compromised systems — often without the target realizing they are exposed.

The creation of an island hopping marketplace is a game-changer, providing attackers with increased incentives to infiltrate systems and a greater ability to embarrass brands, and giving relative amateurs an easy path to inflict serious damage.

**“For executives, the worst-case scenario is no longer the theft of data; it is island hopping, as your brand will be used to attack your customers,” said Kellerman. “This is the dark side of digital transformation.”**

The frequent targeting of educational and government entities illustrates the appeal of decentralized systems that control large amounts of money or information. Thirty-eight percent of IR firms said government was most often targeted by island hopping attacks, compared to 34% for education.

**40%+**  
**OF ATTACKS TARGETED  
VICTIMS THROUGH  
ISLAND  
HOPPING**

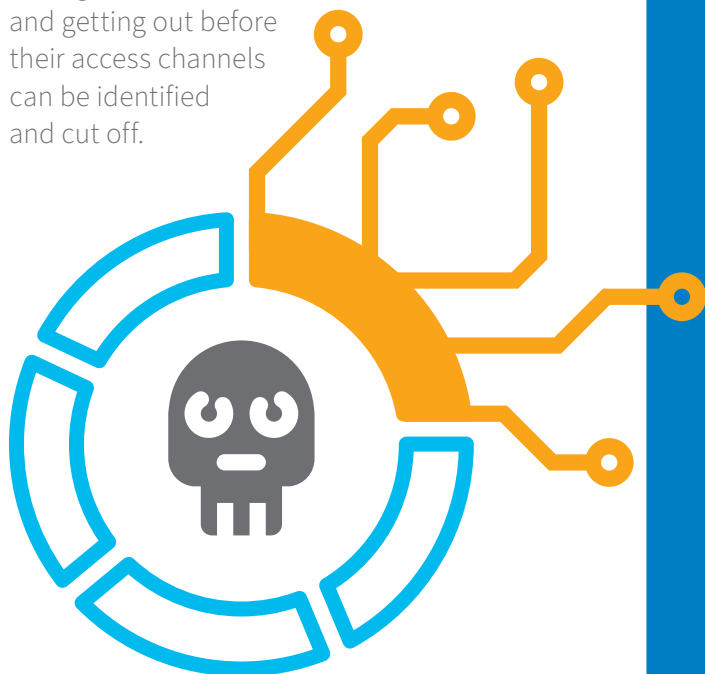


These entities are targeted because they are less likely than corporations to have advanced security controls and 24/7 staffing. Yet they control assets with tremendous value. At research institutions, for example, attacker groups can gain access to research funded by the Department of Defense or National Science Board. In local government, EMS systems, prisons, courts, airports and election systems are all vulnerable to attack.

## C2 on a Sleep Cycle

Once attackers enter systems, they are getting better at remaining there without detections — preferring home invasions to the burglaries of the past. A common mistake by victims is to believe that eliminating malware eliminates the footprint of an attacker.

In our IR survey, 43% of victims saw instances of secondary C2 used on a sleep cycle, up 4% from the previous quarter. This allows malicious actors to evade detection by varying their presence, showing up in different places throughout the network at different times and getting out before their access channels can be identified and cut off.



## WAYS SECONDARY C2 IS BEING DEPLOYED ON A SLEEP CYCLE

When initial C2 is cut off, attackers often deploy a secondary C2 that will jump into action, maintaining their access to the network. Understanding how attackers deploy secondary C2 on a sleep cycle is crucial to stopping it, or at least limiting the damage. Foss explains how these tactics are often being deployed and what firms should be watching for.

- 1 Setting up payloads to beacon out at extended intervals** — such as once an hour, or even once a day — helps attackers remain undetected. Though the traffic from beaconing can be hard to catch, keeping a close eye on the type of data leaving your network — or identifying recurring intervals and packet sizes — can counter the attacks.
- 2 Attackers don't conform to normal business hours**, especially when their day begins as U.S. offices are closing up. For smaller firms without 24/7 security experts or systems monitoring, this means high nighttime vulnerability to C2 and a delayed response when activity occurs outside business hours.
- 3 Larger botnets can deploy multiple C2 callbacks** for different purposes, simultaneously conducting denial of service attacks and data harvesting on the same environment, for example. By spreading out and splitting up their attacks between bots, the traffic looks less suspicious to network monitors.

## Countering via Destructive Attacks

An increase in destructive attacks has seen a parallel decrease in observed incidents of counter-response during attacks, and it's not a coincidence.

The frequency of destructive attacks jumped from 31% in Q1 of 2019 to 41% in Q2. For firms not using endpoint security systems, this makes it nearly impossible to get data on what happened, even with the help of IR experts.



### LACK OF VISIBILITY

Destructive threats explain why **41% of firms said visibility was the top barrier to effective incident response**. And it points to one of the more surprising trends this quarter: Only 23% of victims saw instances of counter-incident response, down from 56% in Q1.

In some ways, destruction is the ultimate in counter-incident response: As a victim calls the police during a home invasion, the attacker decides to burn the house down. Once the house is burnt down, detectives aren't likely to figure out how the thieves broke in or what was stolen, thus erasing the evidence.

It may also be that attackers are getting better at covert counter-incident response. Either way, these trends highlight the importance of using integrated security controls that capture unfiltered endpoint data, so that when an attack does occur, the evidence is safe from the fire.

## Driving Down Dwell Time

As threat actors become better at evading detection, targets need to turn the tables. It's not enough to kick attackers out of your system. You need to hunt them down and keep them out.

With a continued rise in lateral movement — a method that was used in 67% of attacks — victims also need to focus on dwell time as an indicator of reducing damage and destruction risk, and return on investment for security tools.

The opposite is true for attackers. The longer they stay in, the more value they can extract, and they are becoming adept at opening as many backdoors as possible to maintain access, whether that's done using PowerShell, WMI or process hollowing.

"It really highlights the second stage of maintaining and manipulating your footprint in a system," said Kellermann. "It's all about the second phase now."



## Conclusion

As attackers develop communities on the dark web to share experiences and trade in custom tools, defenders need to take the same collaborative approach.

Visibility, the greatest challenge of IR professionals today, is not just about seeing endpoints, but being a part of user exchanges and cybersecurity communities to see the bigger picture.

Financial interests reign supreme, but concerns over our election integrity show how a wide range of verticals are under threat.

Attackers have become dramatically more sophisticated and very well organized. The scale of the threat is growing. The challenge for IR firms and global organizations is to match the cooperation of the adversaries, jointly developing solutions and sharing information that empowers responders to enter each fight with the upper hand.

## About VMware Carbon Black

VMware Carbon Black is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The VMware Carbon Black Cloud consolidates endpoint protection 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, VMware Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 6,000 global customers, including approximately one-third of the Fortune 100, trust VMware 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 VMware Carbon Black's technology in more than 500 breach investigations per year.

*VMware, Carbon Black and vFORUM are registered trademarks of VMware or its affiliates in the U.S. and other jurisdictions. Other trademarks or names mentioned in this press release belong to the respective owner.*

**vmware**® Carbon Black

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

[carbonblack.com](https://www.carbonblack.com)