2020

Security Operations

ANNUAL REPORT

THE LEADER IN SECURITY OPERATIONS

TABLE OF CONTENTS

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

FOREWORD

/// The cybersecurity industry has an effectiveness problem. Every year new technologies, vendors, and solutions emerge claiming to be the final piece of the puzzle. Yet, despite this constant innovation, we continue to see high-profile breaches in the headlines. All organizations know they need better security, but the dizzying array of tools leaves resource-constrained IT and security leaders wondering how to proceed.

We saw this problem magnified in 2020, as security teams everywhere scrambled to secure their environments which featured a newly remote workforce, including the security team itself.

At Arctic Wolf, we believe that the world needs security operations, so we have built a company to do this.

It's also why we've created this report.

Leveraging insight from our experiences, this report will show you key security trends observed by our security operations team, and we'll share some advice on how to advance your own security operations capabilities.

Organizations that embrace security operations are more secure, more resilient, and better able to adapt to changing circumstances like we saw this year. Even as the pandemic completely changed the target environment and impacted the people responsible for protecting it, Arctic Wolf customers experienced no outages in coverage.

That's the security operations difference, and how Arctic Wolf is helping to end cyber risk.

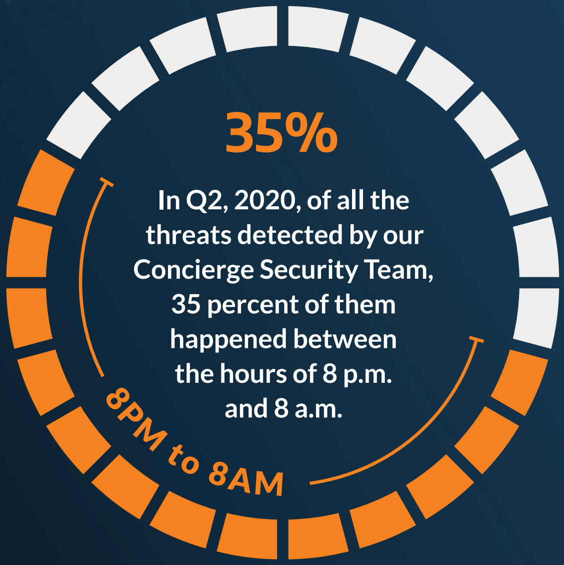
—**Mark Manglicmot,** Vice President of Security Services, Arctic Wolf

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

EXECUTIVE SUMMARY

We've gathered data from the Arctic Wolf® Platform and customer experiences drawn from our Concierge Security® Team to present the key security operations findings and insights from environments protected by Arctic Wolf:

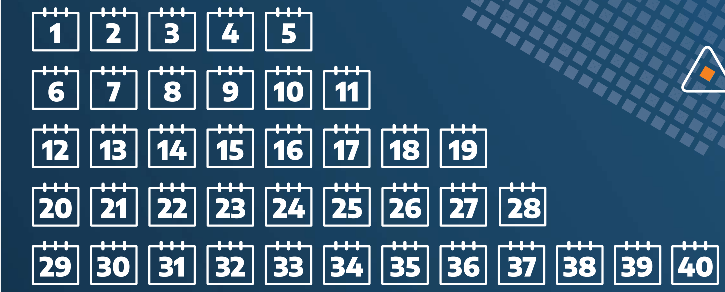
<5 Alert fatigue is a critical issue for the modern-day security operations center and for security professionals. Of the over 100 billion daily observations taken in by the Arctic Wolf Platform, fewer than five validated incidents (with precise remediation recommendations) per week are created for Arctic Wolf customers.



35%

In Q2, 2020, of all the threats detected by our Concierge Security Team, 35 percent of them happened between the hours of 8 p.m. and 8 a.m.

40 Days



The time it takes to deploy patches for critical vulnerabilities increased by an extra 40 days since March. Higher CVE volumes, more critical CVEs, and a disruption of patching programs caused by the dispersed workforce have all contributed to this increase.

64% ↑

Ransomware and phishing attempts detected in Q2 increased by 64 percent over Q1, 2020. This was most pronounced in the banking industry, which saw these threats increase by 520 percent between March and June.

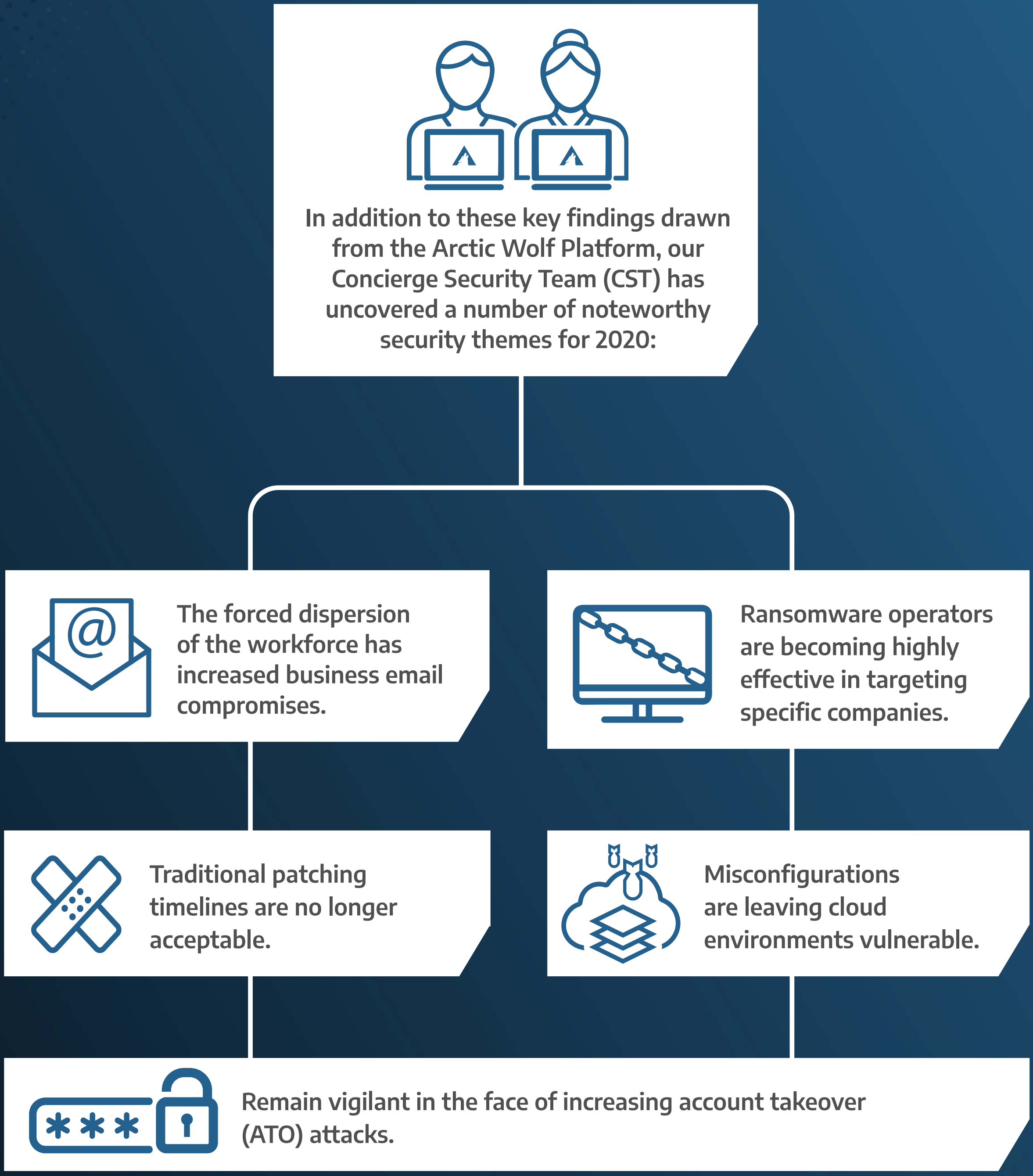
429% ↑

Since March, the number of cleartext usernames and passwords found to be exposed on the dark web has increased by 429 percent.

243% ↑

Since March, the number of connections to open WIFI networks increased by 243 percent. Without proper controls in place, geographically dispersed workforces face increased risks of attacks on unsecured networks.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public



In addition to these key findings drawn from the Arctic Wolf Platform, our Concierge Security Team (CST) has uncovered a number of noteworthy security themes for 2020:

The forced dispersion of the workforce has increased business email compromises.

Ransomware operators are becoming highly effective in targeting specific companies.

Traditional patching timelines are no longer acceptable.

Misconfigurations are leaving cloud environments vulnerable.

Remain vigilant in the face of increasing account takeover (ATO) attacks.

Understanding these discoveries and security themes will better prepare organizations for today's threats while increasing security effectiveness, generating the security operations outcomes they need.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

KEY FINDINGS

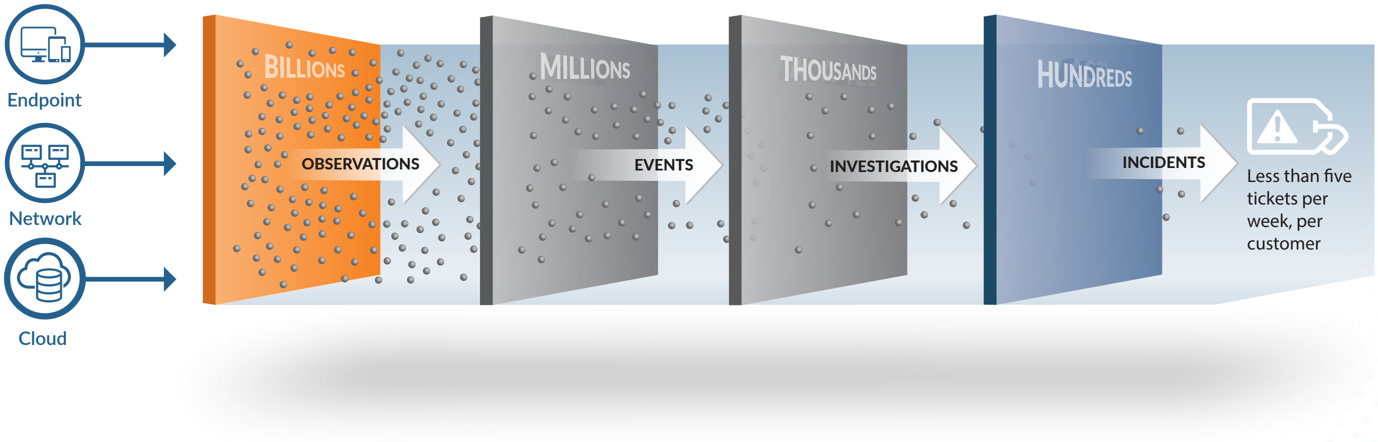
The insight provided in this section represents key findings from the Arctic Wolf Platform. A clear understanding of this information helps to end cyber risk by spotting the most credible new and emerging threats and security trends.

THE END OF ALERT FATIGUE

Most organizations receive thousands of alerts per day from dozens of disparate security tools they've deployed. As they struggle to keep up, fatigued IT and security professionals are forced to increase alert thresholds or turn some alerts off entirely in an effort to deal with the workload they face.

This practice leaves gaps in their posture, increases dwell time of threats, and reduces leadership's understanding of where pain points exist. All of this culminates in making the life of an adversary much easier with respect to how they implement an attack.

Ending alert fatigue is exactly what the security operations approach accomplishes. To quantify this, we reviewed a day in the life of all Arctic Wolf customers to examine how the security operations approach helps teams cut through the noise to get to the right signal. Of the over 100 billion daily observations taken in by the Arctic Wolf Platform, less than five validated incidents (along with precise remediation recommendations) are created for the average Arctic Wolf customer each week. Effective security operations puts an end to alert fatigue.



©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

NOCTURNAL ATTACKERS: MORE THAN ONE-THIRD OF ATTACKS HAPPEN AFTER-HOURS

Stopping modern attacks requires around-the-clock coverage across your entire environment by security operations experts. That's because many high-risk threats come in after-hours, when your employees have left the "office." Attackers look to exploit the path of least resistance, and if no one is watching, they will have hours to operate without the potential threat of true detection.

In Q2 of 2020, 35 percent of all threats detected by our Concierge Security Team happened between the hours of 8 p.m. and 8 a.m.—when most employees and company contractors were off the clock. This was a significant change from Q1, where only 27 percent of threats were observed over the same time period.

This increase coincides with the newly established work-from-home environments resulting from the shelter-in-place mandates from COVID-19. Around-the-clock coverage is essential to ensuring attacks are thwarted after-hours, and when an employee's guard might be down at the start of their day catching up on emails or joining video calls.

Incidents detected by time of day

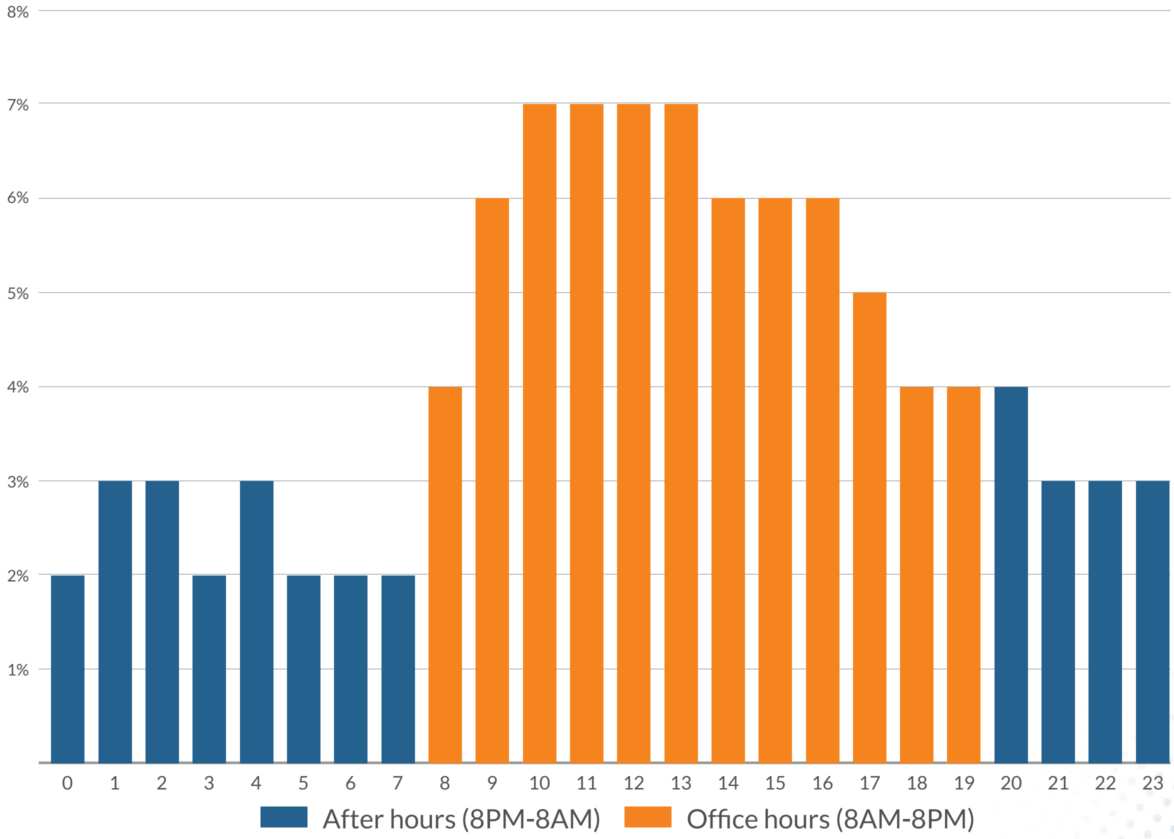


Figure 1: Percentage of total incidents detected by hour of day (January - June)

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Attackers don't respect your evenings or weekends off. In fact, they use these comparatively lax periods to their advantage. Given hours of unfettered and unnoticed access to the environment, they can act on their objectives unimpeded. During the first half of 2020, we observed that 14 percent of threats were ticketed on the weekend (Saturday and Sunday, combined), while the most active day of the week is Friday, when 21 percent of all ticketed threats are observed. While this might appear lower in volume, attacks have a much higher rate of succeeding when your guard is down—especially if you don't have 24x7 coverage of your environment.

Volume of incidents detected by day of week

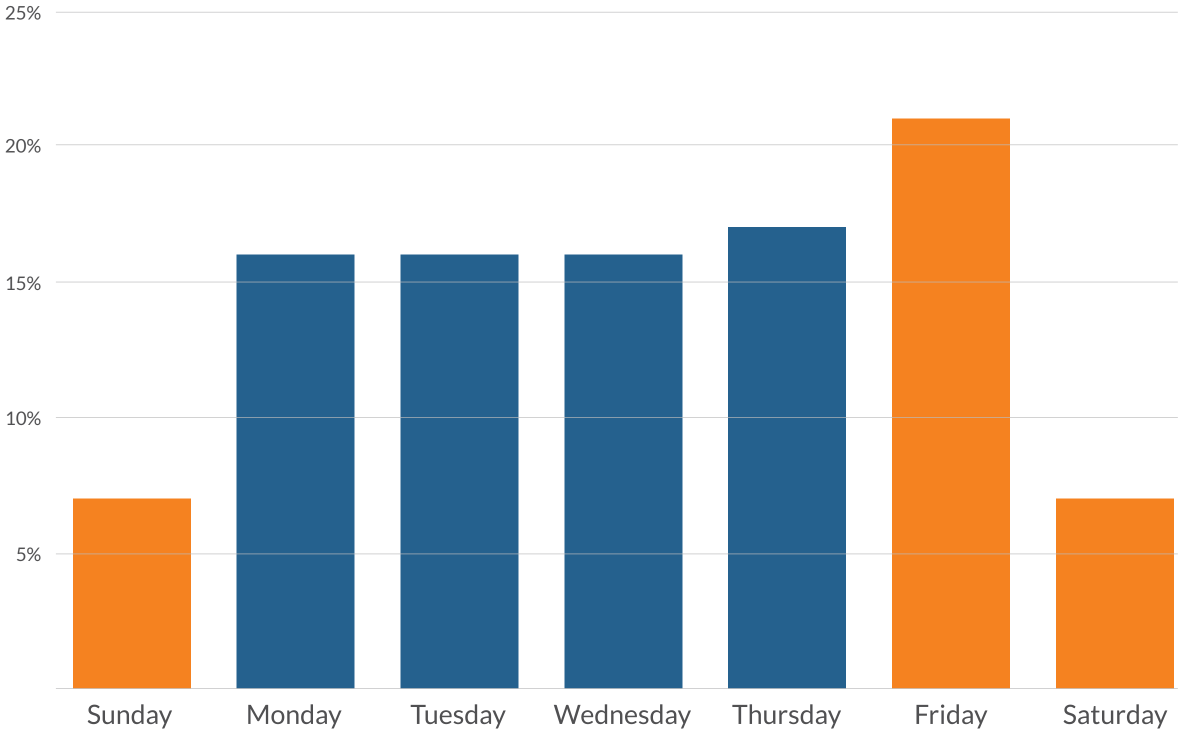


Figure 2: Incidents detected by day of week—January–June, 2020

What can you do?

To properly staff and resource a security operations center on a 24x7 basis requires a minimum of 10-12 people—and that's just accounting for Tier 1 and Tier 2 SOC analysts. These are minimum requirements as it doesn't account for management, system administrators, time spent on detection logic tuning, or other support functions, not to mention illness, vacation, or employee attrition. So, the reality is that you'll need far more personnel to provide complete coverage across your environment. For many organizations, this is an impossibility. So, staffing their SOC becomes a balance of how much work their existing IT personnel can absorb during the day versus how much risk the organization is willing to endure. If adding resources to support around-the-clock coverage feels like too tall of a task, look for partners who can augment your team or provide off-hours coverage.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

UNSECURED WIFI NETWORKS ARE LEAVING THE DOOR OPEN TO ATTACKERS

Devices that connect to open and unsecured WIFI networks (such as those offered at cafés, hotels, or public places) can be particularly vulnerable to attacks since these untrusted networks are open by design to simplify connectivity and authentication.

Since March, we have observed a 243-percent increase in the total number of connections to open and unsecured WIFI networks.

Work from anywhere actually means, “work from anywhere there's connectivity.” Since most remote workers were mandated to shelter in place during this period, this also suggests many home networks are likely open and unsecured.

Average number of connections to open WIFI networks per customer, per month

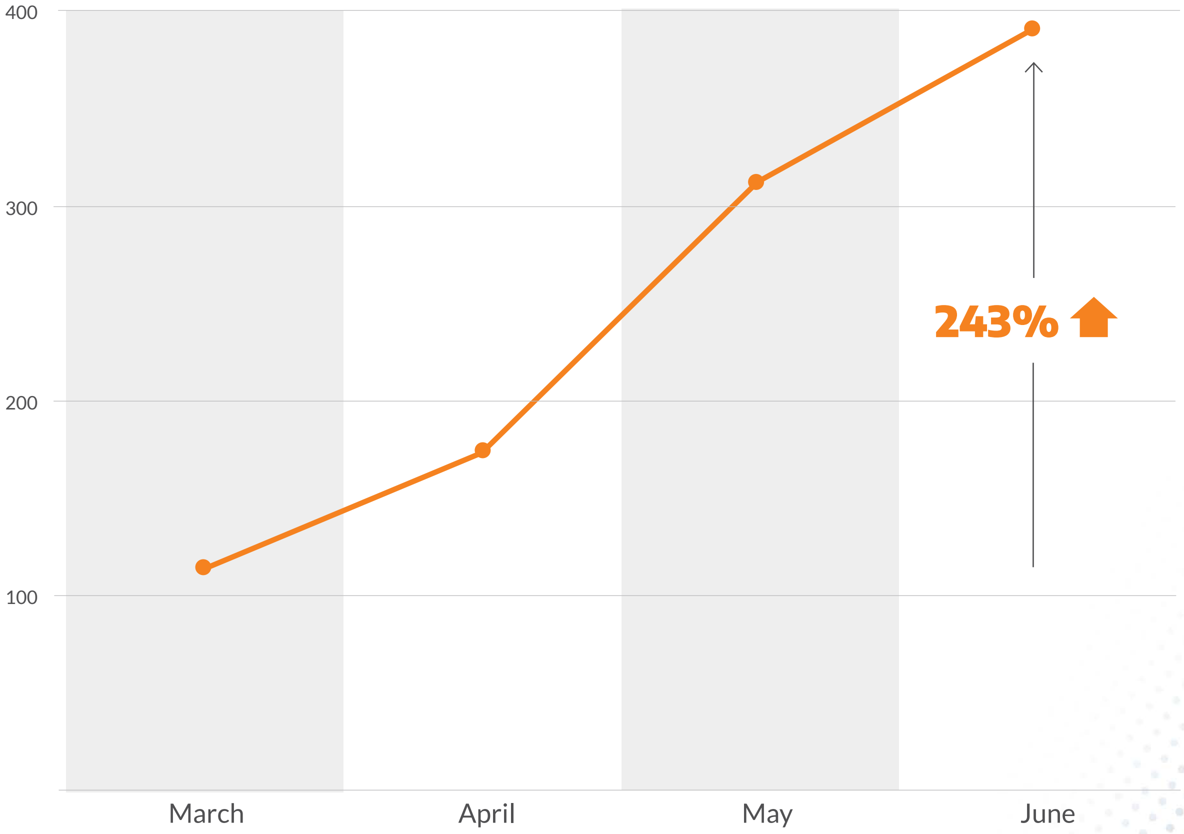


Figure 3: Average number of connections to open WIFI networks per customer, per month.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Attackers use open WIFI networks as an entry point into your corporate environment. They do this by first infecting the WIFI access point or by connecting an attacker system to the WIFI network. Once that is done, they just need to wait for a system to connect. Once connected, a variety of techniques are used to take control of the system or leverage it for lateral movement into your environment. Once such technique leverages the browser's web session cookie. This allows them to authenticate to your internal systems and services without having to know or steal any credentials, instead they just use the web session cookie. This bypasses authentication controls and can grant the attacker broad access to your internal network.

By connecting to an open WIFI network that a user's device has connected to, adversaries can use these stolen session cookies to authenticate to your internal web applications and services.

Without proper controls, an adversary can easily gain access to web applications and cloud-based services without needing to re-authenticate.

What can you do?

The most obvious method is to ensure you connect to WIFI networks that are secure and password protected.

In situations where connecting to open WIFI networks cannot be avoided, the organization should consider deploying a split-tunnel VPN, enabling the user to isolate business applications from consumer applications and connections to the corporate network. Connecting to a password-enabled personal hotspot on supported iOS or Android smartphones can also increase the likelihood of a secure connection.

Endpoint monitoring through an endpoint agent should be implemented to detect and alert to connections to unsecured networks. Keeping software up to date—including antivirus—adds another layer of protection. Finally, in terms of IT policies, browsers and associated tasks should be configured to periodically delete persistent cookies which will push for re-authentication more regularly.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

A PATCHWORK APPROACH TO PATCHING EMERGES

As IT and security operations teams work to re-establish their security perimeter now that employees and contractors connect from home, they've found themselves with few available cycles to patch. Since March, we have observed a major slowdown in patching. It is taking 40 more days to patch vulnerabilities than it did prior to that. We believe this is happening because of the disruption caused by COVID-19, and because there are simply more vulnerabilities to deal with this year (up 23 percent YoY).

Average time to patch critical vulnerabilities

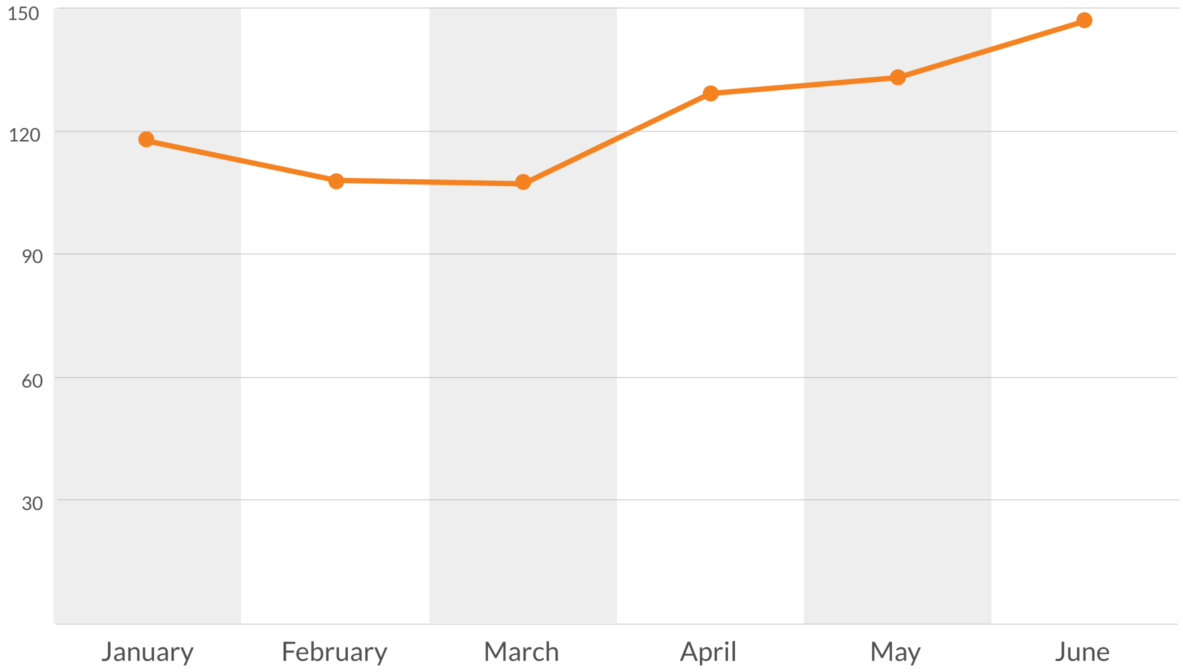


Figure 4: Average time to patch critical vulnerabilities in number of days

With systems now in a more vulnerable state for a longer period of time, organizations are at greater risk of exposure because threat actors now have more time to exploit these systems. Effective security operations helps to prioritize cyber risks and vulnerabilities, so your team is better equipped with complete context on what needs to be patched immediately.

What can you do?

While patch prioritization is hard, it delivers clear results. Proper workflows must exist to ensure that critical risks are assigned to the right individuals within the department to identify, prioritize, and patch exposures as quickly as possible. Don't be derailed by vulnerabilities that cannot be patched for business reasons. Keep tracking and reporting those while maintaining focus on vulnerabilities that can be rapidly addressed. If you struggle with what patches to prioritize, seek security operations assistance to close the gaps on average time to patch, and slam the door on attackers.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

PHISHING WITH RANSOMWARE

Critical threats detected in Q2—such as ransomware and phishing attempts—increased by 64 percent over Q1, 2020. These volume increases seem to coincide with major news events during the COVID-19 pandemic, such as the first confirmed US case, the country's first death, and the announcement of relief benefits. Leveraging current events, attackers also tend to follow the money in their targeting of specific organizations. As such, companies in the banking sector became prime targets for phishing and ransomware, seeing a 520 percent increase in this activity between March and June, which was significantly more than any other industry.

Critical incidents by month

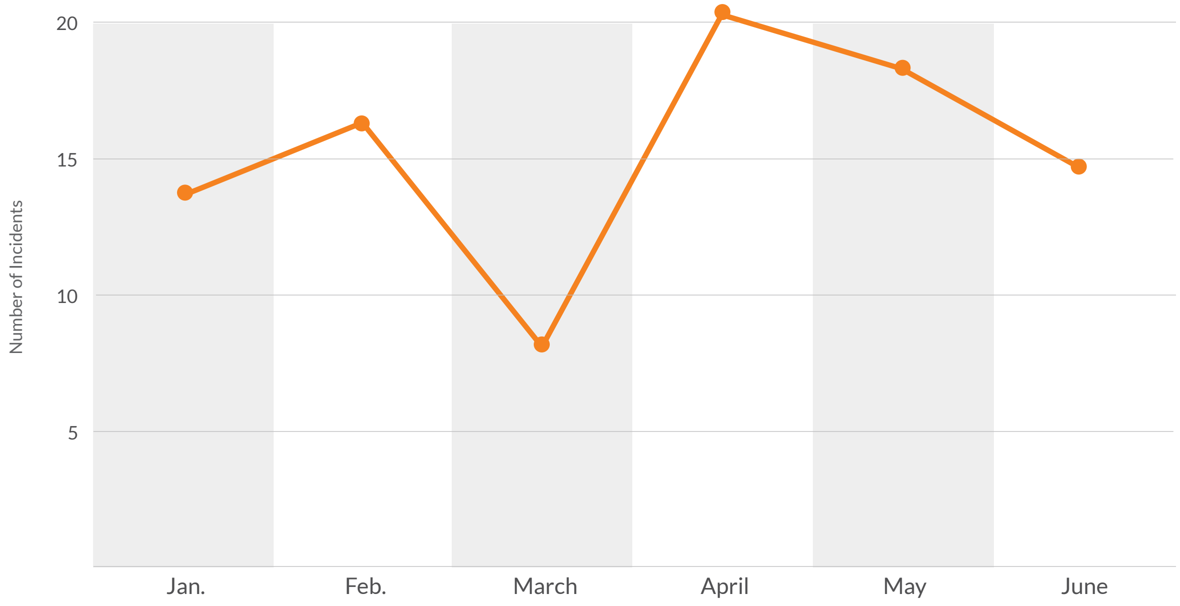


Figure 5: Average number of critical incidents observed per customer by month, January – June

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

COVID-19-related phishing

In Q2, we observed specific examples of how attackers attempted to exploit the COVID-19 situation and use it to their advantage. We saw new, COVID-19-related phishing lures attempt to infect users' systems, steal their data, or infect them with ransomware. Several phishing lure "favorites" that sought to spoof DocuSign and Snapchat, as well as Cerber ransomware threats, were also detected and thwarted by Arctic Wolf.

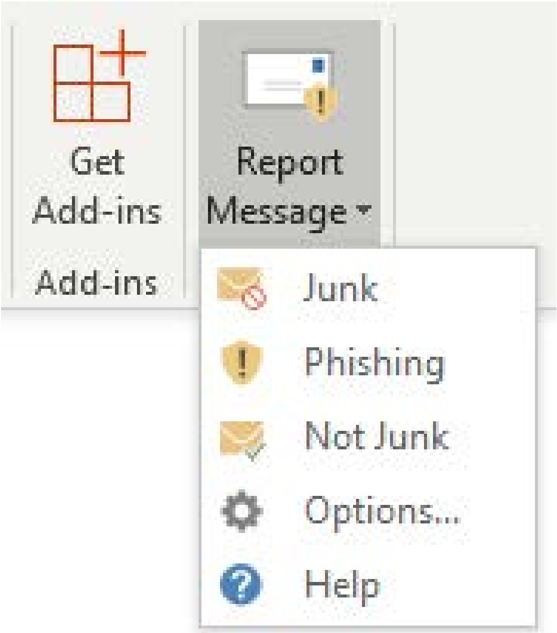
Looking at this trend over the first half of the year, the volume of critical ransomware threats and phishing attempts peaked in April—around the same time as the spike in global COVID 19 infections.

What can you do?

Bad actors are increasingly sophisticated in their targeting, so remain vigilant in the face of new attack tactics, phishing lures, and attack vectors. Reinforce to employees that if you receive a suspicious email, don't click on anything (attachments or links). Instead, use automated tools in your email client to identify the threat and forward it to your IT team for awareness.

When users understand how a phishing attack may attempt to target them, they're better prepared to handle phishing situations. That's why building phishing simulation campaigns into your security awareness training program is a good defense tactic.

Also, your security operations or IT teams should be equipped with run books and workflows to know how to correlate indicators of compromise (malicious attachments, suspicious links, foreign domains, etc.), so you can spot critical threats and address them before they become larger problems.



©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

SHINING A SPOTLIGHT ON THE DARK WEB

If you're not familiar with the term, "account takeover," you should be. This year, we recorded a high-severity account takeover exposure within every single industry vertical that Arctic Wolf protects. These are situations where personally identifiable information (PII), corporate credentials, and other sensitive information makes its way onto the dark web in plain text. This high-value data is bought and sold by threat actors who execute phishing, credential stuffing, and brute-force attacks against the individuals and organizations.

High-severity account takeover exposures by month

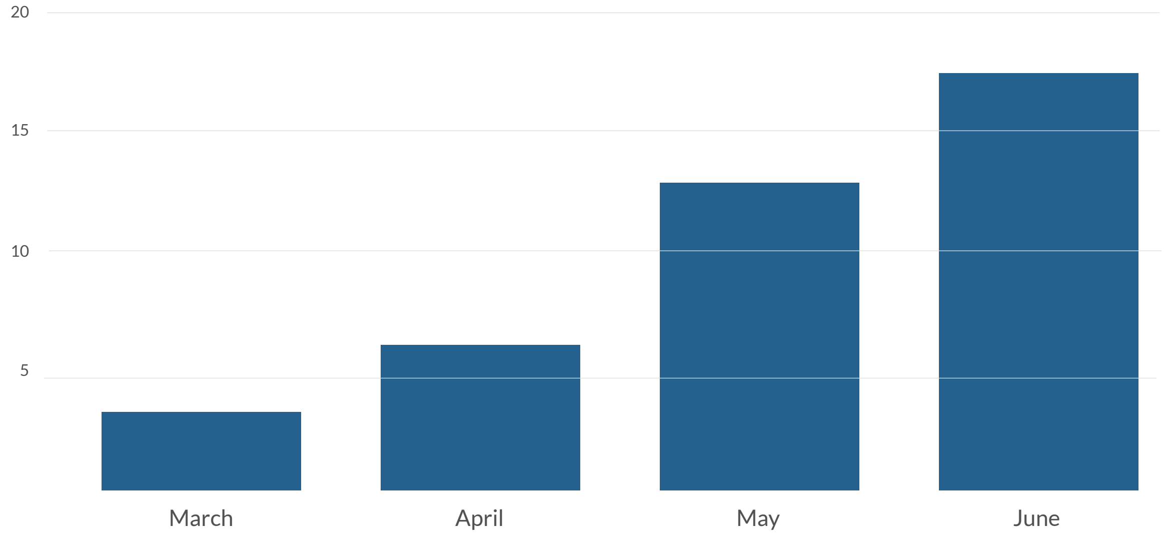


Figure 6: Average number of account takeover exposures per customer, per month (March-June)

And the volume of these incidents is escalating.

Since March 2020, the number of high-severity account takeover exposures detected (where corporate credentials with plaintext passwords were exposed on the dark web) have increased by 429 percent. To put this in perspective, where we were observed an average of three high-severity account takeover exposures per customer in March, that number shot up to an average of more than 17 account takeover exposures per customer in June.

Account takeover exposures take advantage of the fact that password reuse is pervasive, and the use of stolen credentials is the number one hacking tactic for the last several years running. According to LastPass, 91 percent of people know password reuse is insecure, yet 75 percent do it anyway.

This can be a cybersecurity silent killer, as third-party data breaches can leave you exposed without your knowledge.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Getting educated on account takeover

A single breach and new attack vector can severely affect an entire industry vertical. The education sector, in particular, is a recent focus of attackers as remote colleges and universities have created fertile ground for internet mischief. Additionally, new pastes and combo lists (lists of new and previously breached credentials) from various sources have emerged on the dark web, with attackers using these lists and automated brute-forcing tools to test credentials en masse by focusing on specific industries.

These two factors together have made the Education sector an interesting target for attackers. Since March, customers in the education industry have averaged a total of 384 high-severity ATO incidents. This is more than three times higher than the legal, healthcare, financial services, banking, and manufacturing industries combined.

Companies in the healthcare industry make for interesting targets for adversaries seeking to leverage the attention paid to COVID-19 to capture investment, funding, and information coming into those organizations. As the keepers of the cash, financial services and banking companies make for high-value targets, with increased phishing and business email compromise attacks that aim to catch victims off-guard, especially those with weaker than normal security controls in place.

Although the source of many of these breaches remains under investigation, it highlights the importance of remaining vigilant against re-using corporate credentials on third-party sites that are beyond the borders of your organization's protection - especially those sites that serve specific industry verticals.

High-severity account takeover exposures

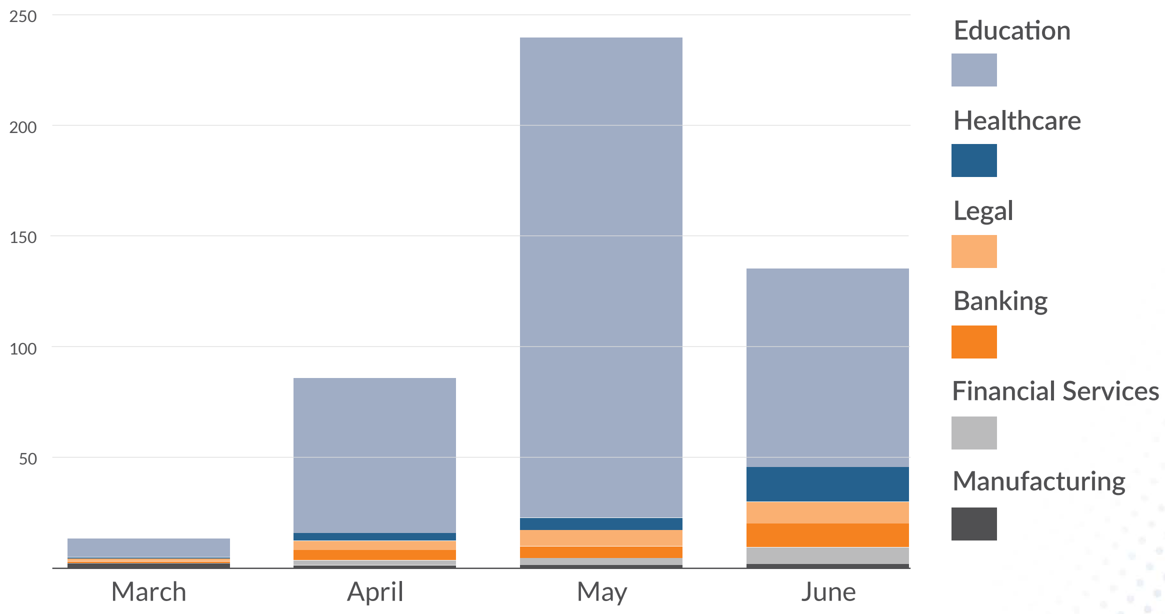


Figure 7: Average number of high-severity account takeover exposures per customer, per month by industry vertical

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

What can you do?

Since password and credential reuse is pervasive across multiple sites beyond the control of the corporate environment, a third-party breach could leave your organization exposed. Consider these best practices and approaches to harden your environment and increase your visibility and awareness of potential account takeover exposures:

- **Acquire visibility into dark and grey web exposures.** Billions of passwords and user credentials are bought and sold on the dark web every day. Brute-force and credential stuffing attacks are often executed through botnets using this information. Look for solutions that can help you shine a light on these dark web exposures, so you can take proper action to change passwords or disable accounts as necessary.
- **Leverage password managers.** Password management software auto-generates and securely stores strong passwords, requiring that the users only needs to recall a passphrase. Password managers also reduce the likelihood that passwords will be reused across third-party sites, since dictionary words and common phrases are not used.
- **Leverage multi-factor authentication.** Enable multi-factor authentication (MFA), especially on your organization's most critical systems. MFA provides additional authentication in addition to the user's credentials, making credential stuffing and brute-force attacks more difficult.
- **Disable/delete expired user accounts.** Deploy IT policies that delete, disable, or expire user credentials for employees or contractors that leave the organization and no longer require access to your systems.
- **Training and awareness.** Simply telling users not to reuse passwords often falls down in practice. In addition to implementing password managers, training and awareness programs should regularly look at password practices and educate users on proper password hygiene.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

KEY THEMES

THEME 1

THE FORCED DISPERSION OF THE WORKFORCE HAS CREATED AN INCREASE IN EMAIL COMPROMISES

Situation

Business email compromises are a lucrative business for cybercriminals because they have a solid success rate with relatively little effort. These compromises focus on taking control of a corporate email account, often by convincing the victim to reset their login credentials. In the first half of 2020, we saw that the forced dispersion of the workforce accentuates the problem because there are far fewer controls in place than when those endpoints are more actively secured behind firewalls on the corporate network.

One such BEC attack thwarted by the Concierge Security Team sought to take advantage of a customer's use of SaaS applications (Office 365). The customer's IT team had taken a very security-conscious approach by enabling MFA across all cloud services, especially O365. In the retail segment, it is not uncommon for this customer to frequently use high-value wire transfers to pay suppliers, merchants, and business customers. The attackers carefully selected their target—an executive whose job included requesting and authorizing major wire transfers. Using a low-and-slow dictionary attack, they focused their efforts on a single email account where their failed logins would not raise an alarm. The attackers got lucky, first by identifying the correct username/password combination, triggering an MFA authentication request which the user mistakenly accepted.

Now, with full access to the account, the attackers were able to perform reconnaissance and cover their tracks. They requested a wire transfer of $700,000 to an account they controlled.

The Concierge Security Team first identified and began to monitor the situation when the account login came from a suspicious country triggering a high-priority alert. The second indicator of compromise came when this suspicious login was quickly followed by a new O365 mail rule that would conceal replies from the accounting department.

With these strong indicators of an attack in progress, the customer's dedicated Concierge Security Engineer immediately contacted their IT security team who was able to get in touch with accounting and put an emergency stop on the wire transfer.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

What to do next?

While it's not a silver bullet, it is essential to enable multi-factor authentication on all accounts. This makes it more difficult for an attacker to compromise email accounts based on credentials alone. In Windows environments, IT admins must recognize that the default protections available through O365 are not sufficient on their own. All recommended best practices (according to NIST and the Center for Internet Security) should be implemented if they are not on by default. Since users themselves remain the weakest link with regards to email compromises, email protection systems like Microsoft ATP, Proofpoint, or Mimecast can help to filter out suspicions files, links, and attachments that can hide attack payloads.

IT and security teams also need to implement proper runbooks and workflows for investigating and remediating email account compromises. At a minimum, emails that originate from outside domains should be flagged with "[EXTERNAL]" to ensure nothing slips through the cracks.

Finally, place effective controls on wire transfer procedures. Business email compromise attacks like these have successfully extorted hundreds of thousands of dollars from victims as these requests appear to come from a trusted source.

THEME 2

RANSOMWARE REMAINS A KEY THREAT TO ORGANIZATIONS

Situation

Like business email compromise, ransomware is now more common as ransomware operators have become more effective attacking specific targets. High-profile ransomware attacks in the recent news include those from Garmin and Canon, and ransomware attacks are not unique to any one industry. Ransomware causes an average of 9.6 days of downtime with an average ransom payment of $36,295. Since infections can come from many attack vectors (RDP compromises, email compromise, phishing, vulnerabilities, etc.), defending against these attacks can be very difficult.

Unfortunately, encryption of data is the last and most visible sign of attack. And usually by this point, the damage has been done. Ransomware attacks are often "low and slow," where an attacker aims to gain persistence in your environment, perform reconnaissance to understand what vulnerabilities exist, and determine their best means of attack.

This year, the Concierge Security Team has observed COVID-19 -themed phishing tactics designed to deliver Ransomware payloads to potential victims.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Ransomware operators are also using traditional families of malware (Ryuk, Cerber, Locky, etc) to infect unsuspecting victims. This is an important reminder that your security teams should be well versed in traditional tactics, while adapting to conditions that introduce new attack vectors.

Finally, moving to more remote environments has required an increase in remote workstation management using remote desktop protocol (RDP). This has led bad actors to increase their use of RDP as an attack vector.

What to do next?

Defending against ransomware infections requires a layered approach to security while operating under the assumption that it's a question of "when," not "if," you will be infected. Since most ransomware operators leverage vulnerabilities and exploits to execute their attacks, practicing good patching discipline—especially with regards to critical systems—is of the utmost importance.

Organizations should also ensure that antivirus systems are up to date with the latest signatures, prevention settings are optimized for ransomware, and should implement immutable storage for their business-critical data and systems to minimize loss and downtime from potential infections. Finally, just having system backups is not enough. Backups should exist offline as well as offsite to be easily recalled in the event of an incident.

THEME 3

TRADITIONAL PATCHING TIMELINES ARE NO LONGER ACCEPTABLE

Situation

The longer a vulnerability goes unnoticed or remains unpatched in your environment, the greater the risk to your organization. Zero-day vulnerabilities are now widely exploited in hours instead of weeks, so a traditional patching timeline of 30 days is no longer acceptable.

The dispersed perimeter has increased the attack surface, pushing out the control of endpoints from inside the corporate network and adding complexity to vulnerability management programs and patching workflows. IT departments also face a 23-percent increase in CVE volumes over the same period in 2019, with a marked increase in critical vulnerabilities identified in the last few months. In some cases, critical RCE exploits found during this time were exploited by bad actors before the exploit was widely announced.

Since March, the increase in the overall volume of CVEs and critical vulnerabilities, along with the geographically dispersed workforce, has added an extra 40 days to the time it takes to patch critical vulnerabilities.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

It is now much more difficult to sift through the alert noise to get to what's important. Organizations must implement a more responsive patch management program to close the gap on critical vulnerabilities before they attract the interest of bad actors.

What to do next

A more responsive patch management program requires organizations to streamline and structure patching, and change control procedures to protect their most critical systems. While complete visibility into vulnerabilities across the environment is required, prioritizing vulnerabilities based on severity and exploitability should guide patching responsiveness. Systems affected by critical and high-risk vulnerabilities should be patched within hours or days, while low- and- medium-risk vulnerabilities can be given reduced priority. Focusing on the most critical vulnerabilities when patching systems will not only reduce the average time it takes to patch critical systems, it also lowers your overall risk score.

THEME 4

REMAIN VIGILANT IN THE FACE OF INCREASING ACCOUNT TAKEOVER (ATO) ATTACKS

Situation

The volume of publicly disclosed data breaches is down year over year. That fact shouldn't lull IT teams into a false sense of comfort that exposures won't continue or that the harvested data is worthless. In fact, our dark web monitoring capability has revealed a major increase in credential exposure. Since March, the number of plaintext usernames and passwords exposed is up 429 percent.

This year, we have detected an ATO attack within every single industry vertical that Arctic Wolf protects.

In a recent example, the Concierge Security Team flagged three breached customer accounts and corporate credentials that were available on hacking forums. After alerting the customer, the Concierge Security Team worked directly with the IT department who initiated password resets to resolve the issue in less than two hours.

One common misconception is that account takeover exposures are triggered as a result of your organization directly suffering a breach. While this may sometimes be true, the pervasiveness of password reuse across third-party sites introduces indirect risks that are much more difficult to spot since they fall outside of your protected perimeter.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

What to do next

While you'll never be able to prevent a breach of a third-party site, you can minimize the impact and the value of the exposed data and limit password reuse by implementing a password manager. Password managers offer secure storage of passwords and don't require the user to remember them individually. This enables your organization to implement stricter password policies that often prevent "personal" user credentials. Many enterprise-level password management applications can also identify users that manage their credentials poorly and may need additional security training/education.

In addition to a password manager, multi-factor authentication (MFA) can block unauthorized access to a user's account should their credentials become known by an external party. This can also act as an early catch to a known credential combination if a user receives a push notification that they did not initiate. In terms of training, therefore, employees must learn to decline and report any MFA push notifications that they don't expect.

Another way to minimize your ATO exposure is to ensure that you have proper offboarding policies and workflows in place for employees/contractors that leave your organization. Credentials that remain active after individuals have left the company create dormant risks – especially if those passwords have been reused elsewhere.

Finally, account takeover exposures are not defects in software that traditional vulnerability management systems can scan for and identify. For that reason, your risk management program should provide visibility into digital risks beyond vulnerabilities.

THEME 5

MISCONFIGURATIONS ARE LEAVING CLOUD ENVIRONMENTS VULNERABLE

Situation

Most organizations don't have the broad visibility necessary to take inventory of their cloud systems or discover cybersecurity risks in their cloud infrastructure environments. What's more, these businesses rarely optimize their configurations to harden their posture and comply with regulations. Cybercriminals know these realities and seek to exploit them.

Cloud providers typically have hundreds of services with thousands of configuration options. While daunting, the Arctic Wolf Concierge Security Team works closely with you to identify and close security gaps within your cloud infrastructure by leveraging the Cloud Security Posture Management (CSPM) scanning capability of the Managed Risk solution.

Here are the most common high-risk CSPM misconfigurations uncovered by the Concierge Security Team within our customers' AWS IaaS environments, and how addressing these misconfigurations will harden your overall cloud security posture:

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Rank	Configuration	Description
1	AWS CloudTrail - CloudTrail Bucket Delete Policy	Ensures CloudTrail logging bucket has a policy to prevent log deletion without an MFA token
2	AWS EC2 - Default Security Group	The default security group is often used for resources launched without a defined security group. For this reason, the default rules should block all traffic to prevent an accidental exposure
3	AWS IAM - Root Hardware MFA	Ensures a multi-factor authentication device is enabled for the root account
4	AWS S3 - S3 Bucket Encryption	Ensures CloudTrail encryption at rest is enabled for logs
5	AWS IAM - Password Expiration	Ensures the password policy enforces a password expiration
6	AWS IAM - Users Password and Keys	Detects the use of more than one access key by any single user
7	AWS EC2 - Open RDP	While some ports such as HTTP and HTTPS are required to be open to the public to function properly, more sensitive services such as RDP should be restricted to known IP addresses
8	AWS IAM - Users MFA Enabled	Ensures a multi-factor authentication device is enabled for all users within the account
9	AWS S3 - S3 Bucket All Users Policy	Ensures S3 bucket policies do not allow global write, delete, or read permissions

What to do next

Organizations need to understand that cloud environments are not automatically secure by default. Settings audits are not a “set it and forget it” strategy or one-time activity. IaaS and SaaS security settings require continuous tailoring and configuring to ensure strong security compliance. The same care you use to secure the perimeter, establish firewall rules, implement MFA, record logs, etc., must also be applied to cloud environments.

To ensure your cloud environment is locked down, look for tools that assist with scanning cloud environments for cyber risks like vulnerabilities, and cloud misconfigurations such as CSPM.

But remember that tools are only as good as the people behind them, who establish workflows to triage and remediate the thousands of alerts that come from cloud environments. Just as cloud environments are not secure by default, a cloud monitoring tool that pushes alerts with no workflow to action them will not solve the problem of hardening the cloud environment if you don’t have security operations experts in place.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

HOW SECURITY OPERATIONS INCREASES EFFECTIVENESS

At Arctic Wolf, we aim to end cyber risk by helping organizations address their security operations challenges. We believe that security has an effectiveness problem, not a tools problem. So, to address this challenge, organizations should consider implementing an in-house security operations center (SOC), or partner with a solutions-based organization that can remove the complexity that comes with building your own SOC.

No matter which road you choose, the following security operations best practices will help to increase your overall cybersecurity effectiveness:

1 Establish monitoring and detection depth across your entire environment

You can't fix what you don't know is broken. And in the case of security, you can't protect what you can't see. That's why the first step in building truly effective security operations is gaining complete visibility across your entire attack surface — users, endpoints, networks, and cloud environments.

2 Develop and implement response service level agreements (SLAs) tailored to high-value assets

Some refer to high-value assets as the "crown jewels." These jewels can come in the form of critical systems, databases, infrastructure, servers, and even people. Establish policies along with SLAs to monitor activity around your high-value assets to help your security operations team better prioritize monitoring, triage, and remediation.

3 Aim for fewer than 10 percent false positives

Without properly tuned detection logic, security operations teams can spend a significant amount of time triaging or threat hunting an IOC only to find that it's not something they should care about. A feedback loop should be put in place that continuously tunes your detection system to know what to look for, and keeps false positives detected to fewer than 10 percent.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

4

Conduct cyber exercises at least two times per year (one tactical — i.e. red team, and one executive tabletop)

Conducting tactical and executive tabletop exercises with your security operations teams helps to elevate the organization's awareness. They should cover the many ways an adversary may attempt to infiltrate the environment, and how to detect and prevent that from happening. These exercises also help harden the environment by identifying gaps in technology and training, while also ensuring that the organization's overall cyber awareness does not go stale.

5

Threat intelligence adds value to daily ops, hunting, and strategic decision making

Augmenting detection technologies and observed security telemetry with threat intelligence brings additional context to support daily threat hunting, operations, and strategic decision making. This intelligence can also help reduce false positives and aid prioritization context so your SOC team knows exactly what to focus on and can ignore the noise.

6

Remediate vulnerabilities based on severity and frequency

As mentioned earlier, the time it takes IT departments to patch critical vulnerabilities has increased markedly since March. Again, this is partly because the dispersed workforce makes patching more difficult, but it also is a consequence of the growing volume of vulnerabilities and digital risks. One of the greatest values that a SOC team provides an organization is increased operational efficiency. Combining several sources of threat and cyber risk intelligence together adds context, which is vital to understanding the severity and frequency of vulnerabilities. Only then can you effectively prioritize remediation, and make the organization operate more efficiently.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

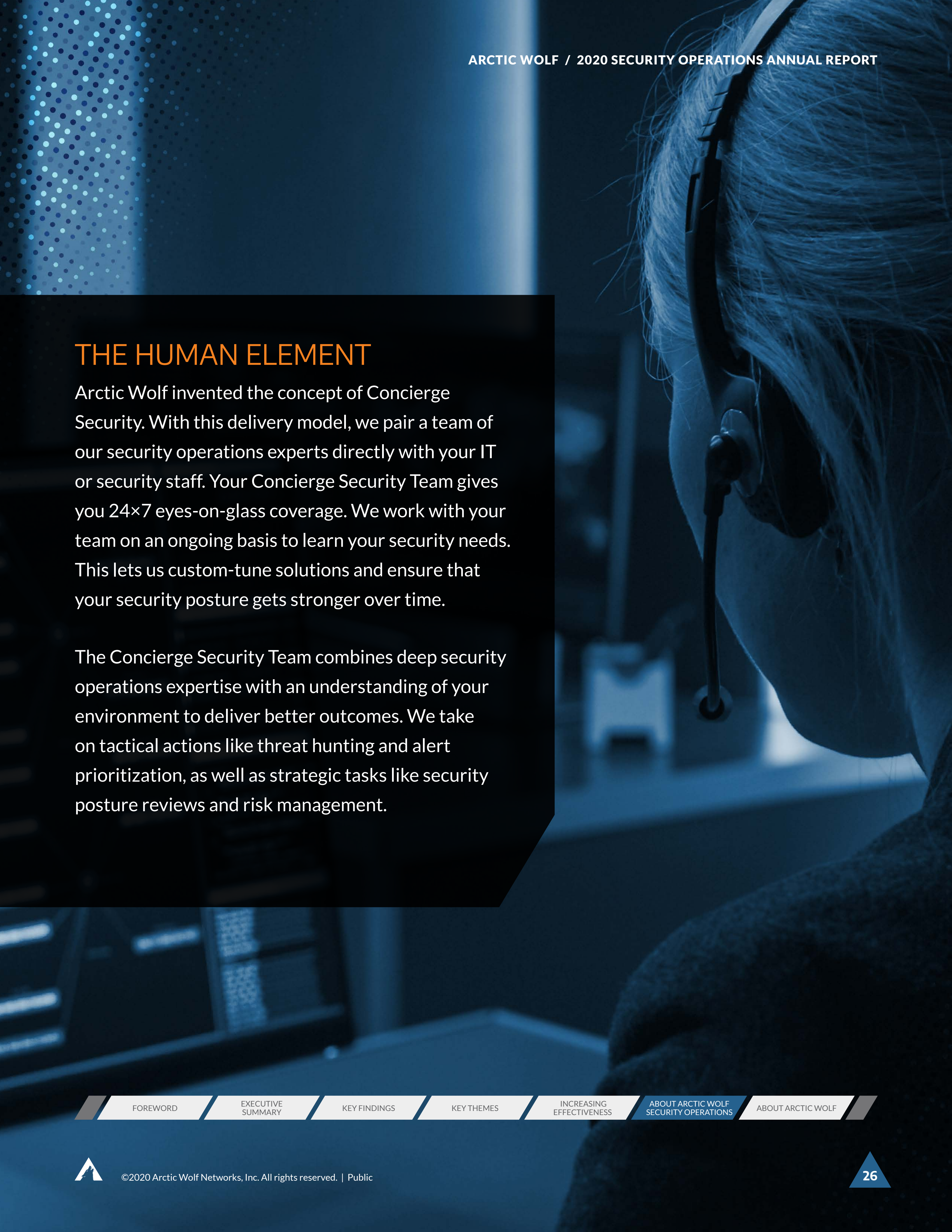
ABOUT ARCTIC WOLF SECURITY OPERATIONS

THE TECHNOLOGY

Spanning thousands of installations, the Arctic Wolf Platform processes over 100 billion security events daily. The platform collects and enriches endpoint, network, and cloud telemetry, and then analyzes it with multiple detection engines. Machine learning and custom detection rules then deliver personalized protection for your organization.

While other products have limited visibility, the vendor-neutral Arctic Wolf Platform enables broad visibility and works seamlessly with existing technology stacks, making it easy to adopt while eliminating blind spots and vendor lock-in.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public



THE HUMAN ELEMENT

Arctic Wolf invented the concept of Concierge Security. With this delivery model, we pair a team of our security operations experts directly with your IT or security staff. Your Concierge Security Team gives you 24×7 eyes-on-glass coverage. We work with your team on an ongoing basis to learn your security needs. This lets us custom-tune solutions and ensure that your security posture gets stronger over time.

The Concierge Security Team combines deep security operations expertise with an understanding of your environment to deliver better outcomes. We take on tactical actions like threat hunting and alert prioritization, as well as strategic tasks like security posture reviews and risk management.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly-trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com

ARCTIC WOLF

CONTACT US

arcticwolf.com | 1.888.272.8429 | ask@arcticwolf.com

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public