Defensive Measures Against Ransomware

Cyber Hygiene Significantly Reduces Small Business Risk

October 2023

GLOBAL CYBER ALLIANCE™

TIDAL CYBER

THREAT-INFORMED DEFENSE

Executive Summary

This whitepaper seeks to quantitatively demonstrate the importance of cyber hygiene – deployment of baseline cybersecurity controls and defensive countermeasures – for small businesses. The analysis is framed around ransomware, one of the most prominent cyber threats facing small businesses today. We take a data-driven approach to building a ransomware "threat profile" specific to small businesses, consisting of top relevant groups and their known attack methods. We then show how deploying baseline defenses directly in line with those top attack methods leads to a measurable improvement in security confidence for a representative small business environment.

In brief, implementing the cyber hygiene measures covered in the GCA Cybersecurity Toolkit for Small Business has a **clear and substantial positive security impact**: our analysis shows that implementing the measures would address (enable mitigation, detection, and/or response to) **72% of the most common ransomware techniques facing small businesses** and 86% of the techniques that enable initial network access or that compromise the confidentiality, integrity, or availability of data. We also outline steps organizations can take to further drive security improvements beyond baseline cyber hygiene.

Primary Author

Scott Small, Director of Cyber Threat Intelligence, Tidal Cyber

Contributors

Philip R. Reitinger, President & CEO, Global Cyber Alliance
Rick Gordon, CEO, Tidal Cyber

The Threat of Ransomware Facing Small Businesses

Ransomware Threat Landscape Trends

Ransomware is one of the most prominent cyber threats facing small businesses today.[1] The U.S. Ransomware Task Force found that **small businesses accounted for 70% of ransomware attacks in 2021**, and our analysis of ransomware extortion threats from 2022 through early 2023 found a similar rate (76%) involving small businesses over that time period.[2] [3]

The potential for lucrative financial gain incentivizes ransomware operators (and others in the cybercrime ecosystem who support them) to opportunistically target a large number and wide range of potential victims. Organizations with inadequate defensive resources (budget, headcount and bandwidth, capabilities, and expertise) are, therefore, relatively more vulnerable to ransomware attacks. This is often the case for small businesses. A survey involving 1,200 U.S. and Canadian small and mid-size businesses found that **many were underprepared for a ransomware attack**: 34% did not train employees on recognizing common ransomware infection vectors, while 30% had no incident response plan (and 35% of those that did had not recently tested it).[4]

Small businesses may also be more susceptible to the financial impact of a ransomware attack. One estimate indicates **an average of 22 days of business downtime as a result of a ransomware attack**.[5] Ransom payments themselves, traditionally made to receive a "key" to "unlock" encrypted data, have risen dramatically in recent years with average payments estimated between $400,000 and $4.5 million (notably, payments are estimated to account for only 15% of total ransomware costs).[6] The rise of the "double extortion" ransomware model in the past three years, where criminals also exfiltrate and threaten to leak sensitive victim data, further exposes businesses to potentially costly data leakage and brand reputation risks.[7]

---

[1] A "small business" is defined here as a business with 500 or fewer employees.
[2] https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf
[3] More details on our methodology for measuring ransomware extortion threats can be found in the next section.
[4] https://cybercatch.com/wp-content/uploads/2022/04/CyberCatch-SMB-Ransomware-Survey-SMBRS-2022.pdf
[5] https://www.acronis.com/en-us/blog/posts/cost-of-ransomware/
[6] https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments
https://www.ibm.com/downloads/cas/3R8N1DZJ
https://www.acronis.com/en-us/blog/posts/cost-of-ransomware/
[7] https://securityintelligence.com/articles/ransomware-double-extortion/

Small Business Ransomware Threat Profile

Ransomware Small Business Threat Profile
"Top" Ransomware with Claimed Small Business Victims: 2022-23

Operation	Claimed Small Business Victims	Small Business Victims / All Claimed Victims*	MITRE ATT&CK® Technique Count
Royal	128	86%	20
Black Byte	42	84%	16
Clop	561	83%	17
Bian Lian	61	82%	26
Play	36	82%	7
LockBit 3.0	481	81%	67
Karakurt	25	81%	26
Lorenz	27	79%	16

*Only includes victims with a documented employee count

Figure 1: Summary of major ransomware operations that claimed small business victims from January 2022 through April 2023

We took a data-driven approach to generating a ransomware "threat profile" specific to the small business sector. A threat profile is a register of relevant, prioritized cyber threats (adversary groups, software, and associated attack techniques) based on quantifiable evidence.[8] Our process involved first identifying which of the myriad ransomware operations in the landscape today pose especially significant threats to this sector, then surfacing which behaviors (techniques) are typically observed during their intrusions. Figure 1 provides a summary of the ransomware operations we included in our threat profile.

[8] https://www.tidalcyber.com/ultimate-guide-to-cyber-threat-profiling

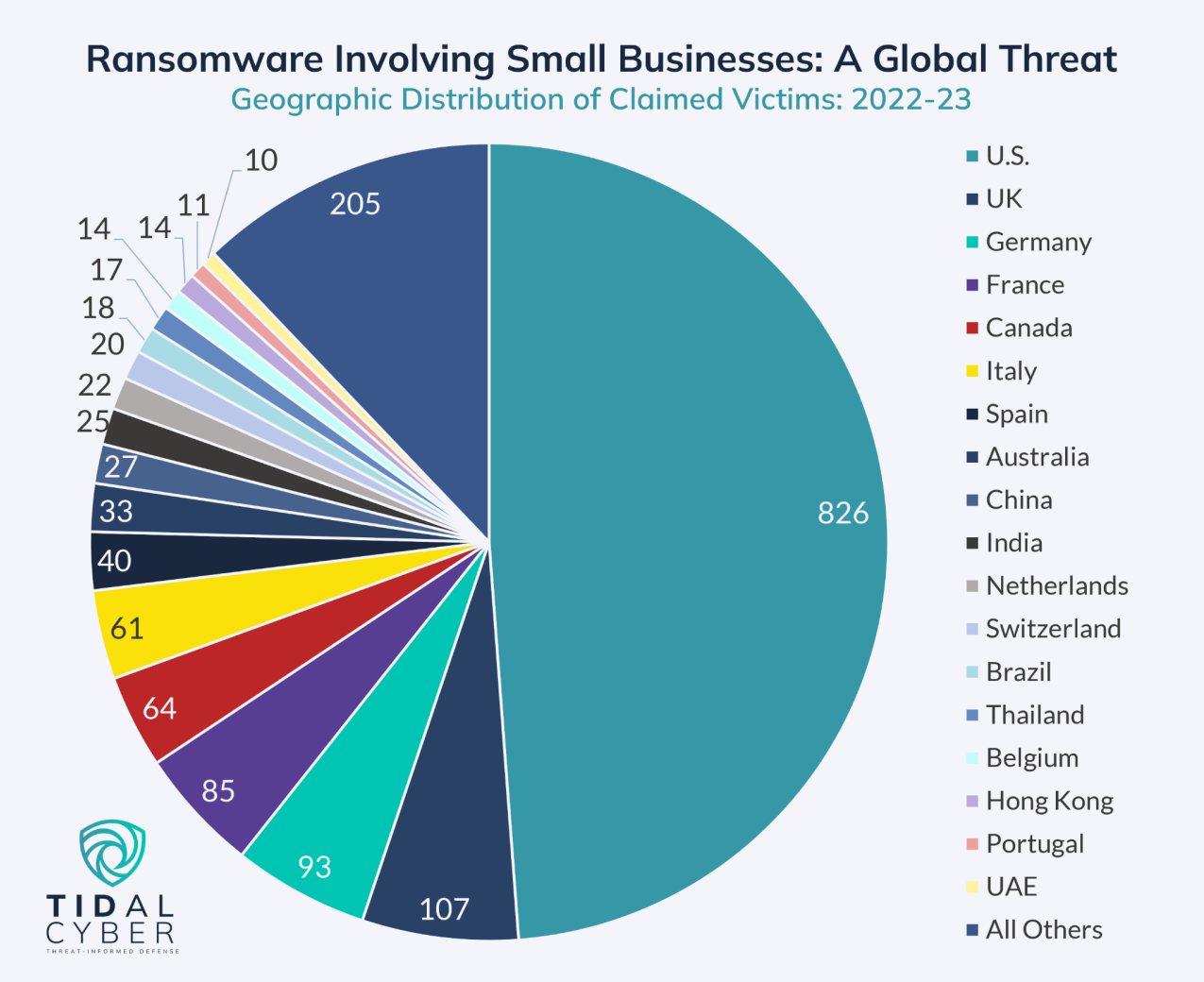

Figure 2: Geographic distribution of claimed small business ransomware victims (the portion for which we could readily identify a likely headquarters location)
January 2022 through April 2023

To identify the most relevant ransomware for small businesses, we needed a consistent set of metrics indicative of victim size. For this study, we sourced a large volume of public ransomware victim extortion claims from the "ransomwatch" GitHub project, which we enriched with victim metadata (size & location) and tallied. In total, **our dataset involved 3,183 public victim claims** from January 1, 2022 through April 30, 2023 that we were able to enrich with an employee count. Of those claims, **76% involved small businesses**. The victim dataset was global in scope (a breakdown for the portion for which we could readily identify a headquarters location is provided in Figure 2).

The average employee count of the small business victims was 101, and the median revenue was $18.1 million. Across the dataset:

- **Fifty-eight (58) distinct ransomware and extortion operations** claimed at least one small business victim during the time period. Fifty (50) claimed multiple victims: 35 claimed 5 victims or more, 25 claimed 10 victims or more, and 10 operations claimed 50 or more victims.
- **Six groups claimed more than 100 small business victims** – in order, they are: **Clop** (561), **LockBit 3.0** (481), **LockBit 2.0** (now defunct) (261), **ALPHV/BlackCat** (176), **Royal** (128), and **Black Basta** (105). For all of these groups, the rate of small business victims relative to all claimed victims was near (and in most cases higher) than the average of ***all*** groups
- Most of the groups operate on a **"Ransomware-as-a-Service" ("RaaS") model**. A rich cybercriminal ecosystem has developed around ransomware, whereby ransomware developers and distributors license the use of their malware to others who compromise victims ("Initial Access Brokers" who resell illicit network access) and those who perform other post-compromise activities, including deploying the ransomware. The RaaS model has lowered the barrier to entry into ransomware attacks and has almost certainly contributed to the rise in ransomware incidents observed in recent years.

For prioritization purposes, we narrowed to the ransomware operations that claimed *especially high tallies* of small business victims and groups with *above-average rates* of small business victims. This provided a **shortlist of eight ransomware families** (seen in Figure 1). In total, **these operations claimed a total of 1,361 small business victims** over the survey period. An average of **82% of their victims** (with an employee count) **were small businesses**. More details on a selection of the shortlisted ransomware operations are below:

- **Royal**: This operation had the highest ratio of small business victims to total victims in our dataset (86%), while also claiming a sizable overall number of small business victims (128). These metrics are especially notable (and concerning) considering the operation is relatively new, carrying out its first attacks in September 2022. In March 2023, U.S. cybersecurity authorities released a joint Cybersecurity Advisory on Royal Ransomware, spotlighting how associated actors have attacked victims in numerous critical infrastructure sectors specifically, including Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.[9]
- **BlackByte**: While responsible for a lower overall number of small business victims in our dataset (42), BlackByte had one of the highest ratios of small business victims to all victims (84%). BlackByte operates as a RaaS and has managed to persist its operations since 2021, including retooling after a decrypter for the malware was released publicly in October of that year.[10] U.S. authorities also acknowledged the threat posed by BlackByte in a joint advisory published in February 2022.[11]

[9] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
[10] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
[11] https://www.ic3.gov/Media/News/2022/220211.pdf

- **Clop (aka Cl0p)**: Clop is an extremely prolific RaaS operation. Active since 2019, Clop actors/affiliates are responsible for thousands of attacks around the world. Clop was responsible for the largest absolute number of small business victims in our dataset (561), and 83% of their total victims were small businesses, a considerably above-average rate. Intrusions involving Clop and associated actors are especially notable since they have featured a variety of attack techniques, including initial access achieved via large-scale spear-phishing campaigns and vulnerability exploits, including exploits involving zero-days. Recent Clop campaigns are representative of a broader trend in the ransomware landscape, where attackers in many cases do not seek to perform traditional file encryption, focusing instead on data exfiltration for the purpose of later extortion attempts.[12]

The Small Business Environment

While the level of cybersecurity inside a small business can vary greatly by size and sector, most small businesses fall below the "Cybersecurity Poverty Line" identified by Wendy Nather as "the line below which an organization cannot be effectively protected. And I've broken down what they're lacking into four categories: money, expertise, capability, and influence."[13] The typical small business network is built at low cost to support necessary business functions, without considering security as a design criterion. The small businesses themselves lack the money to invest in cybersecurity and the expertise to choose security products or services even if money was plentiful. Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), and Cloud Service Providers (CSPs) can help, but only if the service provider includes the most important protections and the small business customers understand the value in purchasing them. In short, simplicity must be a primary goal of small business cybersecurity, with clarity on what are the most important things to do to protect a small business from cyber attacks, especially ransomware, and the business value in taking those steps. Hence, we have developed this paper.

Methodology: Measuring the Effectiveness of Cyber Hygiene Against Ransomware Using the Tidal Cyber Model

Quantifying cyber threats and risks – and the effectiveness of relevant defenses – has traditionally been a challenge for the security community. For this report, we measured the effectiveness of cyber hygiene against ransomware using Tidal Cyber's Confidence Score methodology and the Tidal platform to streamline the analysis. Tidal's Confidence Score represents the confidence that the capabilities in a Defensive Stack will be effective in defending against all the adversary behaviors in a Threat Profile. This section will walk through the elements of a Confidence Score generated for a sample small business facing typical ransomware threats and implementing cyber hygiene as outlined in the **GCA Cybersecurity Toolkit for Small Business**, which comprises free,

[12] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
[13] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m01/breaking-the-cycle-of-security-poverty.html

easy-to-implement tools, resources, and recommendations applicable for any small organization with limited IT expertise, resources, or budget.

Threat Quantification: Small Business Ransomware Threat Profile

The threat profile we generated was based on the eight ransomware operations most relevant to small businesses, derived via the methodology outlined in the previous section. We then pivoted to the techniques associated with these ransomware operations. **Seven of the eight operations included in our profile were not defined in the formal MITRE ATT&CK knowledge base** at the time of our analysis, so we compiled a collection of more than 250 technique references associated with these operations, derived from research into publicly available Internet sources. We added these technique collections as new objects to the Tidal platform.

The collection of techniques that comprise the threat profile can be viewed in Tidal's freely available Community Edition here. Figure 3 shows a summary of the most prevalent attacker techniques observed in this "Small Business Ransomware Threat Profile".

Small Business Ransomware Threat Profile
Top Observed Ransomware Techniques

Technique Name	MITRE ATT&CK® ID	Tactic	Threat Reporting Count	Mapped Log Sources
Data Encrypted for Impact	T1486	Impact	11	6
System Information Discovery	T1082	Discovery	10	4
File and Directory Discovery	T1083	Discovery	10	3
Disable or Modify Tools	T1562.001	Defense Evasion	8	6
Service Stop	T1489	Impact	8	7
Exploit Public-Facing Application	T1190	Initial Access	6	2
Inhibit System Recovery	T1490	Impact	5	5
Phishing	T1566	Initial Access	5	4
Windows Management Instrumentation	T1047	Execution	5	3
Valid Accounts	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	5	3
Network Share Discovery	T1135	Discovery	5	3
External Remote Services	T1133	Persistence, Initial Access	5	3
User Execution	T1204	Execution	4	11
Remote System Discovery	T1018	Discovery	4	4
Modify Registry	T1112	Defense Evasion	4	6
Command and Scripting Interpreter	T1059	Execution	4	5

Figure 3: A summary of the most prevalent attacker techniques observed in the "Small Business Ransomware Threat Profile" developed for this study.

As Figure 3 shows, even when we narrow to the most notable ransomware families affecting small businesses specifically, certain techniques that have been prominently spotlighted in past reporting

on the ransomware landscape appear towards the top of this narrowed list.[14] A summary of some of those techniques is provided below.

- **Initial Access Vectors**
  - **Exploit Public-Facing Application** (T1190): Ransomware actors and associated access brokers perform technical exploits against known flaws in various software as an initial entry point into victim networks. Ransomware actors are known to exploit both newly identified (including zero-day) vulnerabilities, as well as vulnerabilities that have been known for some time, including years-old ones.
  - **Phishing** (T1566): Adversaries send emails and other messages (e.g. via social media platforms) to human recipients, often using social engineering techniques to entice the target to click a malicious link or download and/or execute a malicious file attachment. Phishing for ransomware (and many other modern attacks) can involve complex "execution chains," where several steps occur, often automatically, that lead to the execution of the malicious payload. These chains are typically used to evade defenses.
  - **Valid Accounts** (T1078): Adversaries acquire and use legitimate user credentials to gain unauthorized access to a system. Credentials can be acquired through various means, including phishing, data leaks/dumps, or purchase of stolen credentials on illicit marketplaces, such as those fed by infostealer malware.
  - **External Remote Services** (T1133): This refers to adversaries compromising remote access technology, such as Virtual Private Networks (VPNs), Secure Shell Protocol (SSH), and remote management and monitoring (RMM) servers, to achieve initial entry into a victim environment. Compromise of remote services can be achieved through techniques described earlier, including technical exploit of a vulnerable remote software technology, or use of legitimate remote service credentials.
- **Execution**
  - **User Execution** (T1204): Many attacks still require a victim user to launch malicious software early in the attack chain. Social engineering techniques are often used to trick users into at least opening a malicious file, and in some cases carrying out other interactions that then trigger automated execution chains.
  - **Command and Scripting Interpreter** (T1059): This refers to code interpreters and scripting languages that allow interaction with a computer system. These are often built into systems, but adversaries abuse these features to launch malicious software or directly launch processes that help them achieve their objectives.
- **Achieving Adversary Objectives**
  - **Exfiltration** (TA0010): Ransomware actors use a variety of techniques to exfiltrate data from victim systems. Common methods include movement over command-and-control channels established earlier in an intrusion (T1041). Exfiltration to free or commercial cloud storage services (T1567.002), where traffic

[14] https://www.logpoint.com/en/blog/logpoints-top-ten-mitre-attck-techniques/
https://healthcyber.mitre.org/blog/resources/attack-navigator/
https://www.upguard.com/blog/how-do-you-get-infected-by-ransomware

indicators can blend into benign activity, has been especially popular in recent years. Ransomware actors have been known to extort victims by threatening to leak exfiltrated data after encrypting victim systems, and several prominent operations have moved to exfiltration-only attacks over the past year.

- **Impact** (TA0040): Encryption of victim files (T1486) and disruption of a victim's recovery ability (T1490) have traditionally been hallmarks of ransomware attacks, although some key groups have de-emphasized the technique over the past year, instead monetizing the threat of leaking proprietary or sensitive exfiltrated data.

Figure 3 spotlights the most-observed techniques from our Small Business Threat Profile, in terms of total counts from the public threat reporting we used to generate our profile. Technique "density" (techniques associated with numerous threats in a profile) should be a key input to threat quantification, since successful defenses around those techniques means you are addressing multiple discrete threats at once, providing higher return-on-investment for defensive resources spent.

However, a robust threat profile should include context-relevant threat and technique weightings. While many of the families in the threat profile share certain techniques, others are associated with few or even single families, so weighting the most notable families higher assigns appropriate emphasis on their particular behaviors, without completely disregarding the others' attack patterns. Also, due to factors including definition scope and attack "importance" (e.g., a technique's chances of increasing an attack's spread or impact), certain ATT&CK techniques are more noteworthy than others and should be weighted accordingly. We used Tidal's default technique weighting set, which emphasizes techniques like those just noted, within our threat profile to drive a more nuanced threat score than one based on technique density alone.

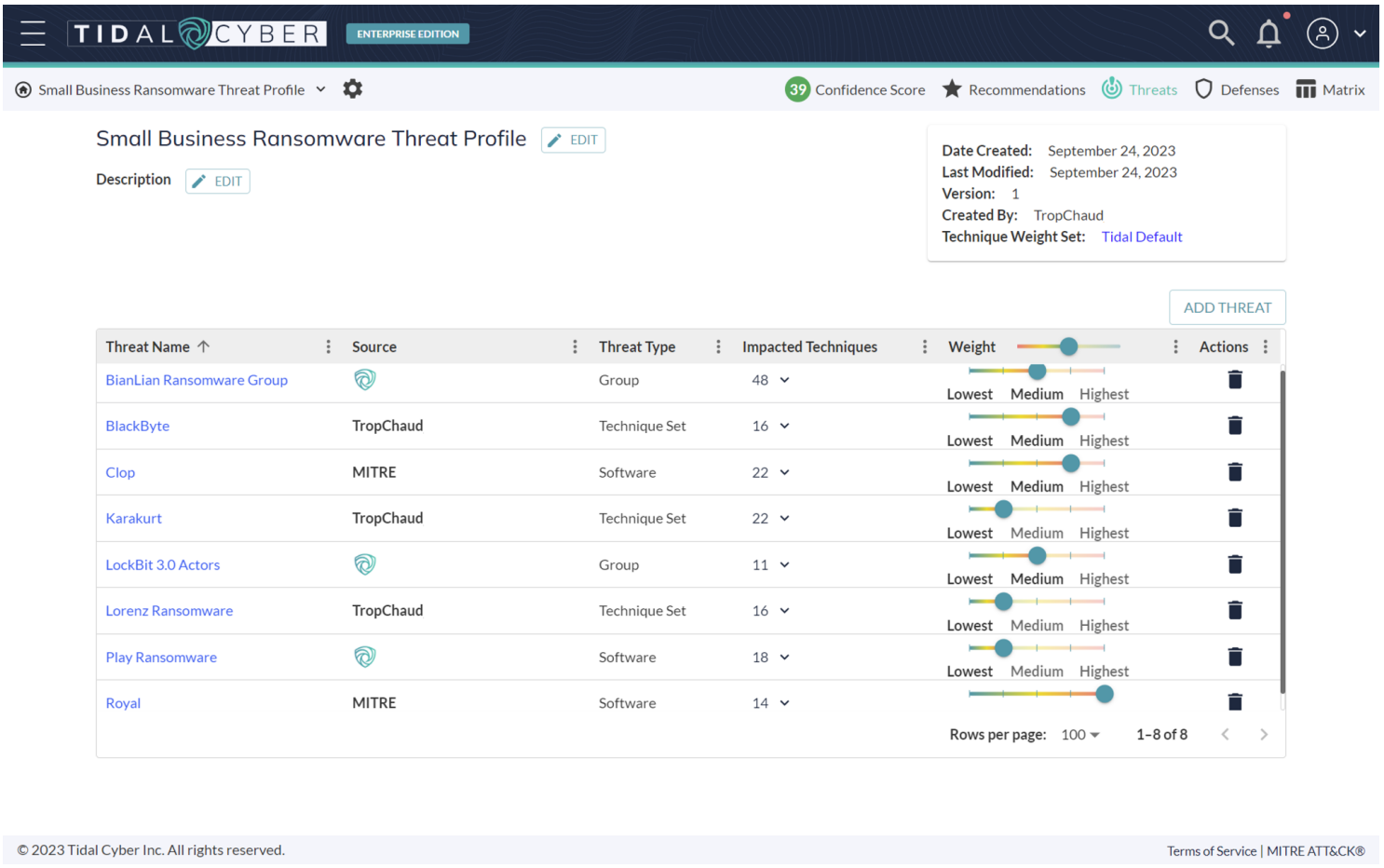

Figure 4: The ransomware operations in our Threat Profile, respectively weighted according to our assessment of overall number and proportion of small business victims.

Quantifying Defenses: GCA Cybersecurity Toolkit for Small Business

A primary strength of the MITRE ATT&CK knowledge base is its position as a common language between the threat and defensive sides of the cybersecurity landscape. Adversary behaviors, as described above, and defensive capabilities, discussed here, can be communicated uniquely defined ATT&CK techniques (each has a unique alphanumeric identifier), unlocking powerful pivoting from relevant adversary threats into discrete defensive controls and capabilities.

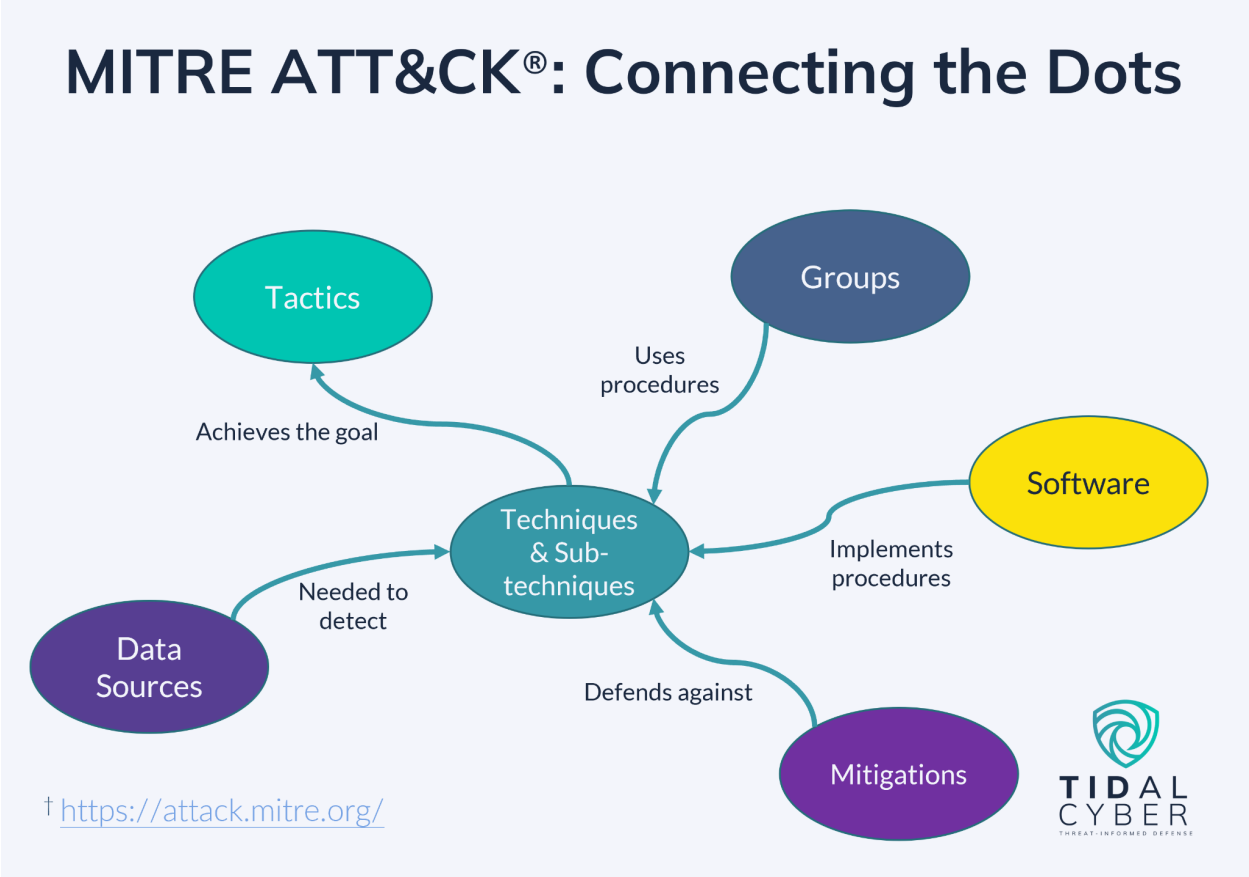

Figure 5: A visual representation of the key elements within the ATT&CK knowledge base and relationships between them, emphasizing the centrality of uniquely defined Techniques & Sub-Techniques.

To quantify the defensive effectiveness of cyber hygiene relative to the Small Business Ransomware Threat Profile, we translated the GCA Cybersecurity Toolkit for Small Business into ATT&CK. The toolkit provides mappings to the Center for Internet Security ("CIS") Controls Version 8.0. CIS in turn provides mappings to ATT&CK Techniques and Sub-Techniques.[15] A matrix summarizing the toolkit mappings to ATT&CK can be viewed in Tidal's Community Edition here.

The toolkit ATT&CK mappings allow us to quantify, via the Tidal scoring methodology, the potential security value of implementing the toolkit recommendations. Defensive capabilities are classified into different categories based on the type of defense they provide. The toolkit mappings represent **Mitigation**, **Detection**, and **Response** capabilities, which we assigned based on the relevant CIS Control "Security Function" to which each GCA toolkit measure is mapped. Other classes of tools and capabilities include **Protections**, **Logging**, and **Testing**. Tidal recommends security teams consider capability types of highest priority to their unique organization and weigh them accordingly

[15] These mappings use Version 8.2 of ATT&CK, released in January 2021. As of writing in September 2023, the current ATT&CK version is v13.

but also assigns "default" weightings, which were used in this assessment and which impact levels of score changes (discussed more in the Analysis and Gaps sections below). Ideally, capability mappings accurately reflect current *configurations* of given capabilities at a given point in time, too.

Quantifying Defensive Confidence

Now that we have defined a threat profile and mapped capabilities into a defensive stack, we can take a quantitative measure of confidence in our defenses. Tidal defines the named combination of a given threat profile and defensive stack as a **Coverage Map**, for the purposes of continually assessing the confidence of those defenses resisting those threats. A Coverage Map answers the questions: "are *my* defenses good enough against the threats *we* care about?" and "where are my gaps?"

The alignment of the techniques in a Threat Profile and the capabilities in a Defensive Stack allows us to take a single quantitative measure of our confidence in our defenses, which Tidal labels a **Confidence Score**. Tidal defines a Confidence Score as the likelihood that your defenses as deployed will successfully defend your organization against the threats you care about. It is a calculated numeric value that represents the confidence that a defensive stack will resist the adversary behaviors in a threat profile.

Best Practices for Building Coverage Maps:

Coverage Maps should be updated to reflect even minor changes in both the threat profile and the defensive stack in a timely manner. While a single overall assessment certainly has value, in practice, organizations will want to assess snapshots of both their overall threats and their defenses, so multiple Coverage Maps are prudent.

Techniques can vary widely among types of adversaries (e.g. espionage-focused adversaries versus cybercriminals like ransomware actors), while different geographic segments or business operating units can have considerably different technology and defensive stacks.

Analysis: How Effective is Cyber Hygiene?

Measuring the Impact of GCA Toolkit Measures Against Common Small Business Ransomware Techniques

According to Tidal's quantification methodology, **implementing the cyber hygiene measures covered in the GCA Cybersecurity Toolkit for Small Business has a clear and substantial positive security impact for the sample small business**, relative to the Small Business Ransomware Threat Profile we outlined for this study. A visual representation of this is provided in Figure 6.

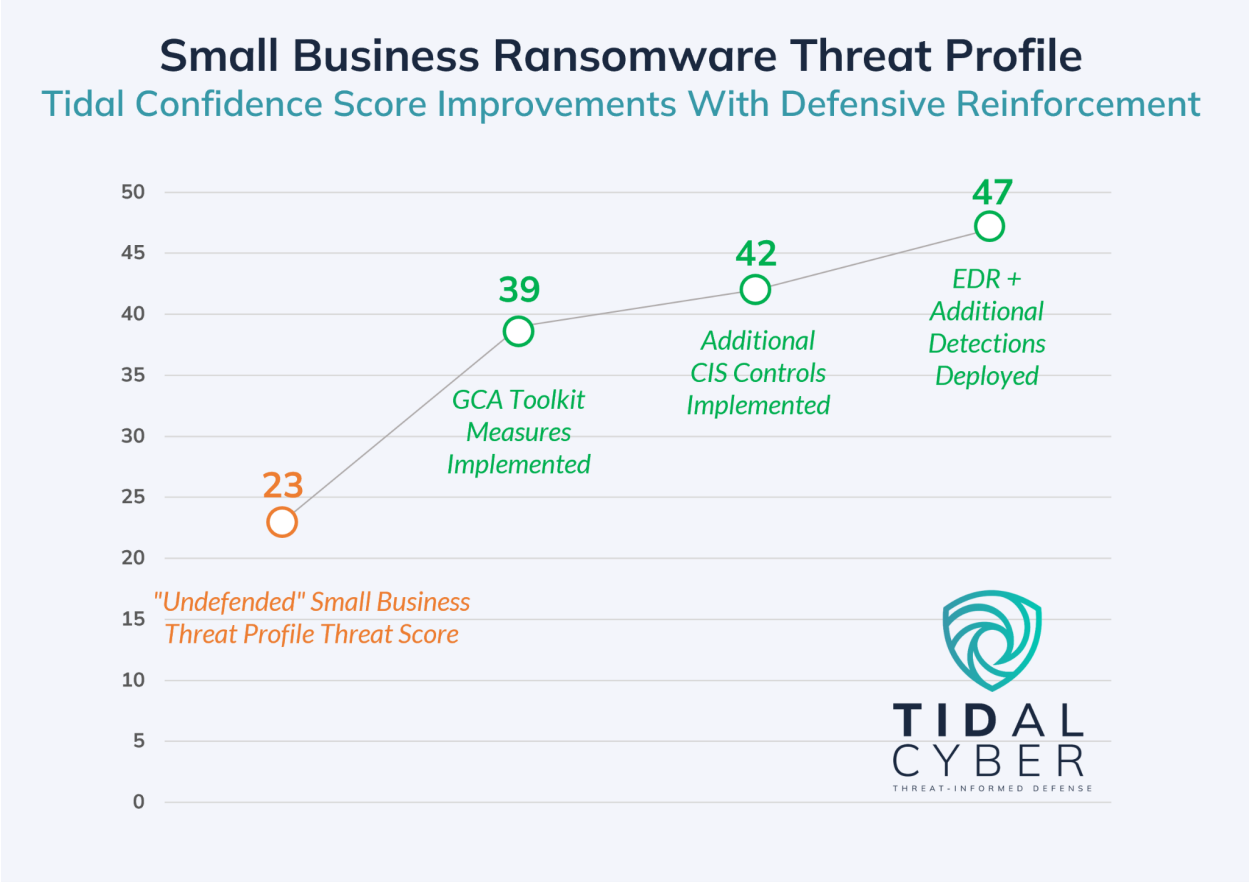

Figure 6: The progression of Tidal Confidence Score improvements, relative to the Small Business Ransomware Threat Profile, as defensive capabilities are progressively implemented.

The sample small business began with a Confidence Score of 23 out of 50 in an "unprotected" state, where no defensive capabilities are enabled (this can be considered the "raw" Threat Score of the Small Business Ransomware Threat Profile). After the toolkit measures were implemented (reflected into the Coverage Map via their ATT&CK mappings), the score increased significantly by 16 points to 39. **This demonstrates that implementing basic cyber hygiene measures – via free tools, resources, and recommendations that are practical for small organizations to implement – has a significant impact in increasing confidence in defending against the most relevant ransomware TTPs.**

The ATT&CK matrix representation demonstrates how **the toolkit mappings overlap with the majority of techniques** from the Small Business Ransomware Threat Profile. More specifically, implementing the measures would address (enable mitigation, detection, and/or response to) **72% of the most common ransomware techniques facing small businesses**, including 86% of the

techniques that enable initial network access and techniques that compromise the confidentiality, integrity, or availability of data.[16] [17]

The number of "capabilities" that are "enabled" when we implement the GCA toolkit measures and the relative importance (weighting) of each capability type influences the magnitude of the Confidence Score increase observed here (from 23 to 39). In total, the GCA toolkit-to-CIS Control mappings represent 44 discrete defensive Capabilities as defined by Tidal, and nearly two-thirds of those are categorized as **Mitigations**, which *proactively* reduce the likelihood and/or impact of mapped adversary behaviors. Acknowledging that various layers of security measures are essential for implementing defense in depth, by default, Tidal weights these Mitigation capabilities more heavily relative to other capability types, like inherently reactive **Detections** and **Responses**, which comprise the other portion of the GCA toolkit mappings.

The following bullets highlight specific toolkit guidance as it aligns with particular, prominent clusters of ransomware techniques:

- **Step 1 – Know What You Have**: Asset inventory is the first step toward mitigating against vulnerability exploits commonly used for ransomware initial access (T1190), including exploits involving remote services (T1133), as well as the real, continued risks of infections via unauthorized removable media devices like USBs (T1091). Tools for device and application identification are provided in Toolkit Steps 1.1 & 1.2
- **Step 2 – Update Your Defenses**: Applying timely patches further drives mitigation against vulnerability exploits (T1190). Steps 2.1. & 2.3 provide tools for keeping devices, applications, and websites up to date and secure.
- **Step 3 – Beyond Simple Passwords**: This step provides tools for strengthening defenses against the myriad credential-related initial access (TA0001) and credential access (TA0006) techniques known to be used by ransomware actors, including abuse of valid credentials (T1078) and brute forcing (T1110).
- **Step 4 – Prevent Phishing and Malware**: The tools provided at this step are especially helpful for mitigating risks by the extremely common ransomware initial access technique of phishing (T1566) and subsequent user-initiated execution (T1204). This step's Additional Training & Resources section also provides several resources relevant to defending against these techniques, such as workforce training resources, a backgrounder, and a sample phishing policy document.
- **Step 5 – Backup and Recover**: This step is intended to help mitigate against traditional ransomware techniques such as data encryption (T1486) and destruction (T1485) and

[16] "Most common" here refers to the 54 techniques – out of the 110 total included in the Small Business Ransomware Threat Profile – that were referenced more than once in our threat intelligence dataset in association with the ransomware groups in the profile (done to limit the impact of potential outlier/uniquely used techniques). Thirty-nine of those techniques (72%) are addressed by GCA Toolkit measures. Techniques aligned with five (out of 14 total) ATT&CK Tactics were considered for the 86% figure: Initial Access, Collection (Confidentiality), Credential Access (Confidentiality), Exfiltration (Confidentiality, Availability), and Impact (Integrity, Availability).

[17] Notably, the Toolkit mappings also cover some techniques beyond the ransomware profile, underscoring how implementation can help defend against techniques that might be used by a variety of other adversary types, such as espionage, hacktivist, or destructive actors.

methods for impeding post-incident recovery (T1490 & T1489). Tools provided include automatic data backup solutions for the popular Microsoft Windows and MacOS operating systems.

- **Step 6 – Protect Your Email and Reputation**: This step provides additional guidance useful for addressing the phishing behaviors (T1566) used by many of the ransomware groups in the threat profile. The GCA DMARC Setup Guide is a free tool to guide your organization through the process of setting up a DMARC policy, as well as additional protections so your organization will have a stronger email authentication mechanism in place to help protect the brand. Step 6 of the toolkit also provides additional DMARC-related training and resources.

Gaps: Where Does Cyber Hygiene End, and How Can Businesses Get More Protection?

As demonstrated above, implementing basic hygiene measures – like those outlined in the GCA Cybersecurity Toolkit for Small Business – can measurably improve confidence in defending against the ransomware techniques especially relevant to small businesses. However, it is worth acknowledging where gaps might remain and considering what steps can be taken to further address those gaps where resources and bandwidth permit.

Notable gaps in the Coverage Map comprising the GCA toolkit mappings and Ransomware Small Business Threat Profile generally fell into two categories. The first was around **endpoint techniques that generally require considerable expertise to detect with high fidelity**. These include certain advanced Evasion techniques and many Discovery techniques, signals of which can be noisy unless detections are properly tuned, a process which often **requires time, resources, and expert knowledge of the local environment's baseline activity**.

The other main category of less-defended techniques were encryption- and obfuscation-focused Command & Control (TA0011) techniques, which must typically be **addressed with advanced network detection & response tools** and/or which often require **significant levels of (and therefore potentially expensive) network-based logging** to observe.

Implementing Additional CIS Controls

To demonstrate that defensive confidence can continue to be increased, we next "enabled" the remaining CIS Controls that do not map to the GCA toolkit, which translated to activating 12 additional Tidal Capabilities within the Coverage Map.[18] These other controls generally come from the higher CIS Control "Implementation Groups", which are designed for organizations to implement as they mature and as their resources grow. Again, the majority of the newly enabled "capabilities" were classified as proactive Mitigations, plus a small number of Detection and Response

[18] Specifically, we "enabled" all of the additional CIS Controls that do not map to the GCA toolkit; specifically, these represent the "Safeguards" within CIS Controls 4, 7, 8, and 12-18.

"capabilities" too. **This step led to a three point additional increase in the Confidence Score.**[19] Figure 7 shows the CIS Controls and Safeguards that pertain to this added layer of controls, as well as the number and types of techniques addressed by these controls.

CIS Control	CIS Safeguards	Number of ATT&CK Techniques Addressed	ATT&CK Tactics Addressed	Associated Threat Profile Ransomware Groups (8 Total)
Network Monitoring and Defense	13.3, 13.4, 13.8	9	Lateral Movement, Command and Control, Exfiltration	6
Penetration Testing	18.2, 18.3, 18.5	3	Discovery, Lateral Movement	6
Secure Configuration of Enterprise Assets and Software	4.1, 4.2, 4.4, 4.5	3	Execution, Discovery, Lateral Movement	5
Continuous Vulnerability Management	7.6, 7.7	1	Lateral Movement	1

Figure 7: Summary of the additional CIS Controls and Safeguards that do not map to the GCA Toolkit mapping (for techniques from the Small Business Ransomware Threat Profile).

The following list provides free tools and resources that align with the CIS Controls referenced in Figure 7:

Network Monitoring and Defense

- **Zeek**: An open-source Network Security Monitoring tool that derives network logs from sensors suitable for analyst review. The BZAR project from ATT&CK enables Zeek-based analytics and reporting mapped to relevant adversarial techniques.
- **Suricata**: An open-source Network Intrusion Prevention System (IDS), IPS and Network Security Monitoring engine. Detection is powered by rule signatures, and regularly updated, publicly available rulesets are available.
- **Snort**: An open-source Intrusion Prevention System (IPS) driven by network packet-focused rules that help define malicious network activity. Community and Subscriber rulesets are available.
- **Sysmon** (System Monitor): Part of the Sysinternals suite of advanced system utilities, Sysmon is a configurable system service that can be enabled on Microsoft Windows operating systems, which provides detailed information about process creations, network connections, and changes to file creation time. Analysis of events generated via Sysmon agents can enable identification of malicious or anomalous activity. Community members have published Sysmon configurations mapped to ATT&CK techniques, enabling easier alignment of events with specific adversary behaviors.

[19] The Confidence Score growth margin is smaller at this step in part because, per Tidal's methodology, the new capabilities (the remaining CIS Controls) provide *additive* defenses around techniques already addressed by measures implemented earlier (the Toolkit).

- **Sigma**: A freely available library of detection rules that can be converted into a large variety of free and commercial security tools' query languages and used for threat hunting and ongoing detection efforts.

Penetration Testing

- **Atomic Red Team**: A freely available library of offensive security unit tests designed to replicate adversary behaviors within an environment. Each test is aligned with an ATT&CK Technique or Sub-Technique, facilitating pivoting and testing around relevant adversary behaviors. For example, there are eight Atomic Red Team tests mapped to the Network Share Discovery Technique used by six of the eight ransomware operations in the Small Business Ransomware Threat Profile.

Secure Configuration of Enterprise Assets and Software

- **auditd**: The Linux Auditing System. Configuring auditd to expose relevant ATT&CK mappings can provide alignment of audit events with adversary behaviors.

Continuous Vulnerability Management

- **Nuclei**: Nuclei is a "Fast and customizable vulnerability scanner based on simple YAML based DSL [domain-specific language]". "Nuclei is used to send requests across targets based on a template, leading to zero false positives and providing fast scanning on a large number of hosts."

Other Resources

- **Dissect**: "Dissect is a digital forensics & incident response framework and toolset that allows you to quickly access and analyse forensic artefacts from various disk and file formats, developed by Fox-IT (part of NCC Group)."
- **osquery**: An operating system instrumentation framework for Windows, OS X (macOS), and Linux that allows users to more easily explore operating system data. osquery can be used to hunt for threat behaviors, and configurations can be mapped to ATT&CK to expose relevant adversary techniques.

Implementing Additional Defenses (EDR & Detections)

As a final step, we added a representative endpoint detection and response (EDR) tool to our Defensive Stack and also added and enabled an additional layer of **Detection** capabilities, represented by Sysmon (referenced in the list of resources above). In total, this final step saw a relatively large number of additional Detection capabilities enabled within our Coverage Map: more than 1,000 from the representative EDR and another 100+ from Sysmon. These capabilities provided additive defenses for a large majority of the Threat Profile techniques addressed by the GCA toolkit and CIS Control ATT&CK mappings, plus defenses for techniques not yet addressed via the GCA or CIS measures, especially in the Discovery, Defense Evasion, and Persistence

ATT&CK Tactics and to a lesser degree the Collection and Privilege Escalation Tactics. This caused the Confidence Score to increase yet another five points, to a total of 47 out of 50, representing a robust overall posture.

At this point, the sample organization has implemented many security measures, and curious readers might wonder what steps can be taken to reach a score of 50. The EDR capability mappings used representative default configuration states, where most Protection capabilities (which prevent or lower the likelihood and/or impact of mapped behaviors) were turned off by default, while a small number of ATT&CK techniques remained unaddressed by the controls and capabilities in this Defensive Stack.[20] Enabling those disabled capabilities and implementing defenses or mitigations for the remaining techniques would likely drive the score even higher. We also want to emphasize that the methodology is not designed to suggest that an organization is "done" with security if they reach a high Confidence Score, even a 50 – adversaries regularly modify their behaviors, and technology (even security tools and their configurations) changes, at times unexpectedly, necessitating regular re-evaluation of defensive confidence as often as resources and bandwidth permit.

Recommended Next Steps for Public Interest Cybersecurity

Three recommendations are immediately apparent from this study.

- First, implementation of basic cyber hygiene is extremely effective. Free tools like the GCA Cybersecurity Toolkit and others are available. However, are there means to make deployment of cyber hygiene even easier, such as by building controls into the services offered by MSPs, MSSPs, and CSPs? The less we ask those below the cybersecurity poverty line to do, the better off we will all be.
- Second, implementation of additional measures identified in the CIS Controls can further reduce risk. Examples of such controls include Network Monitoring and Defense, Penetration Testing, and Secure Configuration of Enterprise Assets and Software, which help especially address ransomware Lateral Movement and Discovery techniques. GCA should examine if there are ways to help small businesses implement these controls.
- Significant further reduction of risk is provided by EDR and advanced detection tools. Can tools or models be devised that make implementing these measures feasible for small businesses? For example, could advanced detection be effectively implemented with a lightweight device or agent that is automatically updated by a shared service? Solutions to address this problem have been proposed before but not widely deployed among small businesses.

[20] Specifically, three Defense Evasion Techniques – Debugger Evasion (T1622), Time Based Evasion (T1497.003), Environmental Keying (T1480.001) – and three Reconnaissance Techniques, which are typically carried out outside the visibility of the target organization, making detection difficult.

Conclusion

The need for widespread cyber hygiene measures has never been more clear. We know the steps that small businesses and even individuals need to take to substantially decrease their risk from cyber attacks, including ransomware. A substantial and continually growing body of free and easy-to-implement cybersecurity resources now exists (many of which are aggregated in the GCA toolkit), lowering the barrier to achieving cyber hygiene (and even more robust security postures).

Now, we need to have the political and economic will to ensure the necessary steps are taken. The return on investment is obvious.

globalcyberalliance.org
tidalcyber.com

Copyright 2023 Global Cyber Alliance & Tidal Cyber