WHITE PAPER

FIGHTING FIRE WITH FIRE

Stopping SMB Attacks Using Tools Sized (and Priced) for the Job

NETWORK DEFENDER

CELERIUM.com

LOW-HANGING FRUIT

An experienced burglar can undoubtedly penetrate a home security system given enough time and commitment. But rather than expend substantial effort to rob the house with the alarm system, most thieves would likely choose to rob the house next door, the one without any defenses.

Seasoned pen testers can compromise just about any network given enough time and resources, but even those with little experience can penetrate poorly protected enterprises using freely available tools.

We've learned over the past few years that cyber criminals view the world through this kind of opportunistic lens, particularly when it comes to attacking the SMB (Small and Medium Sized Businesses) community. If professional cyber attackers from the Russian GRU, China's PLA Unit, or North Korea's Bureau 121 want to compromise just about any enterprise network, it's very unlikely they can be stopped indefinitely. If an enterprise spending hundreds of millions of dollars is still at risk from sophisticated attackers, then the local roofing supply company, regional trucking provider, or 5-attorney law firm wouldn't have a chance.

Fortunately, state-sponsored cyber criminals are focused with much more ambitious objectives than attacking the police department in a 10,000-person town in the midwest. Unfortunately, this does not spare the SMB community from the threat of cyber crime. In fact, there are countless cyber criminal entrepreneurs that see the SMB as a potential cash cow, largely unprotected and easy to target with broad, commoditized automated attacks that probably would be much less likely to work against a larger company. The logic is disturbing for the SMB community, but solid for the attackers: when they can use the same server to target thousands of businesses and get a success rate of 10%, cyber criminals can profit handsomely with little to no effort. Returning to our alarm system analogy, this means those houses without an alarm system are an easy mark, and will eventually be exploited.

"71% of ransomware attacks target small businesses, with an average ransom demand of $116,000 Attackers know that smaller businesses are much more likely to pay a ransom, as their data is often not backed-up and they need to be up and running as soon as possible."[1]

THE SMB ATTACK METHODOLOGY

When a nation-state actor targets a large private or government organization, the attack can take months to plan, involve weeks of probing, reconnaissance and extensive research, target specific individuals, leverage obscure vulnerabilities or spear phishing, and require multiple, highly-skilled cyber attackers. If you've never reviewed the MITRE ATT&CK Framework - you really should - it is a fascinating piece of work (**see: https://attack.mitre. org/**) that details attack methodologies observed over time by cyber bad actors.

While the same processes exist in attacks on the SMB, it is much, much easier to achieve success in that community, as evidenced by the countless number of hacks and ransomware incidents we see hitting the SMB every day.

[1] https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/

It is easier because SMB systems and networks will never be defended the same way an enterprise network can be. This comes down to simple economics of time, money, and people. To build a sophisticated security program that takes into account all of the stages of the attack lifecycle is no easy effort. Because of this challenge, cyber criminals can be highly successful leveraging widely available tools to identify targets with glaring vulnerabilities, and in the largely unprotected SMB world, there are no shortage of options for the bad guys. Take, for example, a port scanning tool called masscan[2], available free of charge on Github, that can "scan the entire Internet in 5 minutes." Cyber criminals can use tools like this to identify open ports on networks anywhere, essentially unlocked gates that can form the foundation of successful attacks.

HOW?

No software is perfectly coded. As applications increase in sophistication, and are integrated with other complex software systems, flaws or gaps in security are inevitable. The flaws are called vulnerabilities, and the US government's National Institute of Standards and Technology (NIST) tracks them. Called Common Vulnerabilities and Exposures (CVEs), they are ubiquitous, and growing, totaling over 18,000 reported in 2020, or about 50 per day.[3] CVEs can be the genesis of cyber attacks when "exploits" for them (small executable software programs that take advantage of vulnerabilities) are created and sold, often on the dark web.

Exploits for many CVEs require exposed ports to be executed, which is why port scanners like masscan are essential tools in the hacker's toolkit. Thus, attackers identify a vulnerability - often those recently discovered and unlikely to be patched by their targeted victim - scan for the port or ports running the vulnerable software and version, and attack the organizations satisfying those criteria...a process that's nearly 100% automated.

So, when you learn that a local chain of lumber yards was the victim of a ransomware attack, it wasn't because the attackers meticulously surveilled the lumber yard's network, or laboriously researched its employees to exploit a social media tidbit tied to an obviously-guessable password. No. The lumberyard was simply one of several entities that happened to have deployed the vulnerable software version, and it's network configuration presented the port scan characteristics that enabled the chosen exploit to be effective.

As they say in the mob movies: "it's not personal, it's just business."

As an SMB or an MSP that serves SMBs, there are some stark realities to contend with in this discussion. First, with tens of thousands of vulnerabilities in deployed software today, and 50 new CVEs being introduced daily, it's impossible to plug all the holes. Second, if your business is connected to the Internet - and which one isn't in 2021? - you're being scanned and probed for open ports and the vulnerabilities that lie behind them, probably much more often than you might expect.

"As attackers increasingly automate attacks, it's easy for them to target hundreds, if not thousands of small businesses at once. Small businesses often have less stringent technological defences, less awareness of threats and less time and resource to put into cybersecurity. This makes them an easier target for hackers than bigger organizations."[4]

[2] https://github.com/robertdavidgraham/masscan
[3] https://www.securitymagazine.com/articles/94602-record-number-of-critical-and-high-severityvulnerabilities-were-logged-to-the-nist-nvd-in-2020
[4] https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-faceand-how-to-stop-them/

But, the good news is that, as an SMB, it's highly unlikely you're being specifically targeted by sophisticated bad actors, but rather the attacks for which you're most vulnerable are automated and impersonal. And, automated attacks are easier to stop - or catch quickly - than those launched by sophisticated threat actors.

"...cybercriminals can launch thousands of digital attacks designed to compromise your operations at every turn, only one of which ever needs to connect to cause serious disruption."[5]

THE BAD GUYS' ACHILLES HEEL

More good news. Cyber criminals can't avoid a fundamental truth about the Internet: every attack must originate and be controlled from a computer (port scans, phishing emails, post-compromise command and control/telemetry), and, the corollary to this rule is that every computer on the Internet has an address (IP). When attacks are launched from an IP address, eventually threat intelligence services are alerted that that address is the source of malicious activity, and that information spreads relatively quickly these days, limiting the efficacy of that attack source...at least for organizations subscribing to - and leveraging - threat intelligence.

Sophisticated cyber criminals with deep pockets (like the nation-state actors mentioned in the opening to this paper) can stand up new infrastructure from which to launch complex attacks, thwarting threat intelligence operations for extended periods, and giving them time to execute the kinds of high profile attacks we hear about in the popular media. These kinds of well-heeled organizations can avail themselves of other techniques to mask their attack IPs as well, at least for a period of time.

But as we discussed previously, the Russian military is not attacking the local Pediatric Dentistry practice. Individual threat actors are. And they often use known-compromised infrastructure (IP addresses already on threat intelligence block lists) for their automated attacks.

WHY?

First, they don't have the resources to mask their origin like nation-state actors, but more importantly, they don't have to. If they can scan the entire Internet in minutes, there will be an ample supply of potential victims with networks unprotected against even attacks originating from well-known compromised IPs. Cyber criminals are immoral, but they're not stupid. They know it's much more efficient, and lucrative, to find a poorly defended target than to waste time and effort compromising a small business with even basic cyber defenses.

BUT I HAVE A FIREWALL...

Many SMBs assume that their firewall will protect them against attacks originating from compromised IP addresses, and they're right...if their firewall is properly configured and actively managed. But that can be filed in the easier-said-than-done folder.

[5] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

There are millions of high risk IP addresses on the Internet, and thousands of new ones reported or deemed risky every week, so it's nearly impossible for an SMB to keep up. Add to this tsunami of potentially compromised devices the reality that all firewalls have a limit on the size of their blocklists, and it's easy to conclude that firewalls alone are a poor defense against even unsophisticated, automated attacks common in the SMB community.

IF YOU ONLY HAVE ONE BULLET TO FIRE

It may sound like a threadbare aphorism these days, but the best defense against any cyber attack is a layered approach. Forcing the bad guys to penetrate multiple defense rings to access sensitive data is a best practice no expert would dismiss. But, that's another item for our burgeoning easiersaid- than-done folder. Typical SMBs don't have the resources or expertise to build, let alone maintain and operate, a multi-layer cyber defense system, and outsourcing the installation and maintenance of such a system is cost prohibitive.

The key is to match the defense to the threat. It's far too expensive to bring a 50-caliber machine gun to a knife fight, but it's foolish to bring just your bare knuckles to that same knife fight. There are solutions on the market today that provide highly affordable, exceptionally effective protection against the kinds of automated attacks common in the SMB community. Network Defender, for example, delivers a 100% automated, threat detection and blocking solution priced for the SMB community, and for the MSP channel that exclusively delivers it. Effectively, it's a fully managed firewall without any human intervention, the kind of clever and efficient automation needed to counter similarly automated attacks.

STARTING WITH THE OBVIOUS

As emphasized previously, no single cyber security solution is impervious to attack, and the more layers of defense that can be affordably installed, the better. But for the SMB community, often operating on razor-thin margins, stopping the bad guys before they can get a foothold on the network is by far the most well-informed approach. Blocking connections from devices with poor reputations is not only a good start, but given the relatively unsophisticated threats that confront the SMB community, it can provide a degree of protection that far outstrips its cost.

ABOUT CELERIUM

Celerium® powers active cyber defense solutions to help protect organizations and communities from increasing cyberattacks. With a rich 16-year history of facilitating cyber threat sharing for critical industry sectors and government agencies, Celerium is an established leader in providing innovative cybersecurity solutions, with solution directions based on the evolving needs of the industry.

Learn more at **www.Celerium.com** and follow us on X at **@CeleriumDefense**

CELERIUM.com