dark3

ATTACKING THE GATEKEEPERS

The first comprehensive analysis of attacks against the Managed Service Providers on the front lines of today's cyber battlefield

A Dark Cubed Analytical Report
January 2020
https://www.darkcubed.com | @darkcubedcyber

ABOUT THIS REPORT

This report represents a first of its kind. We analyzed network traffic from firewalls deployed at globally distributed Managed Service Providers (MSPs) to get an accurate perspective about the level of threat faced by these critical service companies. The results are gravely concerning. After months of careful analysis, it is evident that there are multiple active campaigns revealing a deliberate, systematic, and ever-increasing barrage of attacks launched against MSPs by malicious actors and criminal organizations. The answers provided by the security community to date are woefully insufficient; spending more money is not the answer. It is time to wake up to the reality that we have entered a new era of cyber risk in which the gatekeepers are under siege, and once they fall, their clients are easy prey.

dark3

Dark Cubed would like to extend a special "thank you" to the team at GreyNoise. The data developed by GreyNoise provides valuable insight into the noise of the Internet and was heavily utilized by Dark Cubed to prepare this report.

INTRODUCTION

This report summarizes the findings from Dark Cubed's detailed analytical review of MSP network traffic, representing a set of globally distributed Managed Service Providers.x

KEY FINDINGS

- 100% of MSPs participating in the study suffered from both automated and directed attacks.
- 6.9% of the traffic impacting MSP networks is related to bots, scanners, and hackers.
- Geofencing is not an effective countermeasure on its own because adversaries simply purchase hosting space in "friendly" countries.
- Cloud hosting does not guarantee security: 31% of the hosts associated with Digital Ocean were seen performing suspicious or malicious actions.
- Attacks primarily focused on exploiting Windows Remote Desktop, followed by insecure remote access, file transfer, and hosting services.
- A single MSP suffered a botnet attack comprised of 20,000 unique IP addresses from 149 countries, sourced from 3,607 different organizations.
- MSP defenses are overwhelmed by friendly fire associated with companies that routinely scan for information gathering; 66% of the monitored MSPs were scanned by Arbor Observatory, followed by Shadowserver Foundation and BitSight.

6.9% *percent of traffic impacting MSP networks came from bots, scanners, and hackers.*

100% *percent of MSPs targeted by malicious actors.*

160,613 *number of verified malicious hosts observed attacking MSP networks*

dark3

EXECUTIVE SUMMARY

We are in a new era of digital risk. In the United States, over 40,000 MSPs serve over 64% of the Small and Medium Business (SMB) market [1]. As criminal actors grow more sophisticated, it is becoming increasingly clear that they are picking out targets that give them a bigger return on their investment of time and energy. MSPs are being targeted as a result. When an attacker exploits one MSP, they have the potential to access the data that every customer of the MSP maintains with little to no extra work. The FBI and U.S. Department of Homeland Security have repeatedly warned MSPs and their technology platform providers about such attacks. If an MSP is compromised by ransomware or another cyber attack, their end customers will also be compromised.

Our platform automatically collects anonymized network data for analytics, and we decided to explore this data to see what we could learn about the present and growing threat against MSPs and their customers. Based on our findings, our CEO, Vince Crisler, described this as a "new era of cyber risk." He expounded: "What we are seeing today is a level of organization and sophistication that we have previously not seen from malicious actors focused on MSPs."

100% of the MSPs we studied were directly targeted and attacked. This number cannot be overstated. There are active, systematic, and purposeful attacks underway to gain access to MSP networks and the networks of their customers. These attacks are launched from around the globe and from all of the major cloud service providers. Many attacks can likely be traced back to both nation-state actors and criminal syndicates, although attribution is not the purpose of this report. As a result, geofencing and singling out certain nation-states is not enough to protect against malicious attacks. It takes a far more robust security solution than simply pretending that part of the world doesn't exist.

Common remote access tools increase risk. Remote access tools used by MSPs to support their customers present the greatest risk to a network due to the number of fatal vulnerabilities associated with this functionality. Last year we saw countless MSPs compromised through Remote Desktop and Remote Monitoring and Management (RMM) tools commonly used to manage their client's networks. Huntress Labs performed great work in 2019 proving RMM tools were being weaponized for ransomware delivery [2], and reports from news outlets, such as Reuters [3], articulate that nation-state hacking against cloud and managed service provider infrastructures are on the rise.

[1] https://www.comptia.org/content/guides/comptia-buying-guide-for-managed-service
[2] https://www.reddit.com/r/msp/comments/c2wls0/kaseya_weaponized_to_deliver_sodinokibi_ransomware/
[3] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

Attackers target MSPs for one simple reason. Gaining access to an IT service provider's network grants trusted access to their client networks. From a hacker's perspective, spending a few days penetrating an MSP and gaining access to dozens or hundreds of customers is a far more efficient use of time than attacking small and mid-sized business companies directly. As we move into 2020, we fully expect this trend to continue and the pace of attacks to increase rapidly.

MSPs are overwhelmed. Although MSPs and their software providers have generally improved their defenses as a direct result of the increased attacks seen in 2019, successful exploits have continued. The MSP industry now faces a "crisis of credibility," and the daunting task of walking the line between communicating their cybersecurity value proposition while not proposing cost increases that cause their customers to explore other service providers' offerings.

To put this in perspective, a single MSP we examined was attacked by a botnet consisting of nearly 20,000 unique IP addresses, representing 149 individual countries and 3,607 different organizations. Once you understand the effect of the volume and intensity this targeting has on an MSP, it becomes clear that one mistake, one misconfiguration, could prove fatal.

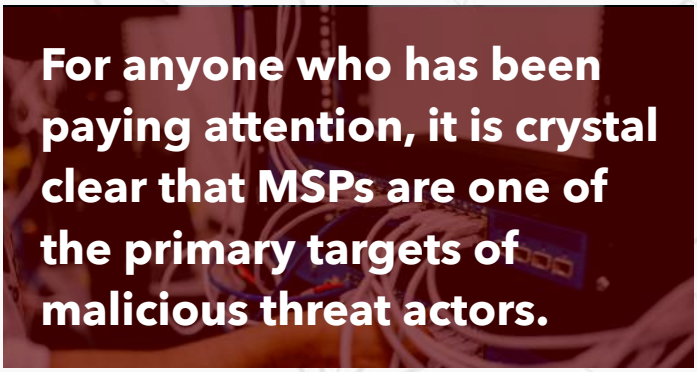
Fighting a losing battle. A cyberattack on one MSP is devastating for all MSPs. This loss of confidence and credibility cripples the industry and hurts business for all in the channel. A 2018 CompTIA report reports that 64% of small businesses were using one or more IT services from one of the 40,000 MSPs in the United States. According to one MSP CEO, who wished to remain anonymous, "We are fighting a losing battle."

Managed service providers must reorient their business strategies to reflect the fact that they are now operating in an environment where any mistake, any error in a network configuration, is likely to result in a breach.

THE MSP CHALLENGE

MSPS ARE UNDER CONSTANT ATTACK BY MALICIOUS ACTORS

MSPs are increasingly under deliberate and systematic attacks by malicious actors and criminal organizations. The average MSP manages the networks of dozens—if not hundreds—of smaller businesses. From an attacker's standpoint, compromising one MSP is like getting an all-access pass to thousands of small and medium enterprises. Attackers are leveraging stolen credentials, malware implants, and phishing attacks to infiltrate MSPs and, by extension, their clients' networks. A successful attack can have wide-reaching effects that impact the MSP first and then ripple out to the MPS's clients, eventually impacting the customers of those clients.



ZDNet described one alarming example of such attacks in a recent article [1]. Hackers were able to gain access to remote access tools used by MSPs, which they then used to spread ransomware to the MSP's end clients. Other organizations are reporting that hackers are weaponizing RMM tools to deliver ransomware. It is abundantly clear MSP networks represent the first and most important line of defense when it comes to protecting their clients.

In another report, Huntress Labs discovered that RMM tools were being weaponized for ransomware delivery [2]. To make matters worse, we continue to see disturbing reports from news outlets such as Reuters that nation-state hacking against cloud and managed service provider infrastructures are on the rise [3]. There can no longer be any doubt that if you are one of the more than 40,000 MSPs in the US and over 60,000 MSPs globally, then you are being targeted by sophisticated attackers.

Throughout our rapid growth over the last year, we have had many detailed discussions with an increasing number of MSPs who are well aware of this threat. Unfortunately, their hands are tied by the cost and complexity of traditional cybersecurity solutions in the market today. The average security solution can take hours to deploy, weeks to learn, and months to reach full efficacy.

To put it bluntly, if you are an MSP supporting the IT infrastructure of a small business with operating expenses that are stretched to the limit, it is nearly impossible to convince your customers to double or triple their spending to get a basic level of security.

Try explaining to a customer who just invested in a firewall, that although they are better protected than they were before, their new firewall is not going to protect them from persistent attackers. While people might try to argue with this statement, it is clear from looking at any large enterprise that has invested hundreds of thousands of dollars—or even millions—into security infrastructures; they don't expect a firewall to provide a clear line of defense. Instead, they make those investments to augment already existing firewalls with additional analytics, log aggregation, threat intelligence integration, and for human analysts to parse alerts and "hunt" for threats. Deploying a firewall without regularly updating the rules, tuning the configuration, and monitoring operations is functionally useless over time. As time goes on, the security provided will degrade until the firewall's only value is a false sense of security.

MSPs require an effective, easy to operate, rapidly deployable system that can provide immediate interaction with the firewall to counter emergent threats.

[1] https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/
[2] https://www.reddit.com/r/msp/comments/c2wls0/kaseya_weaponized_to_deliver_sodinokibi_ransomware/
[3] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

STATE OF THREAT

AN OVERVIEW OF THE OBSERVED THREAT ENVIRONMENT FOR MSPS

Dark Cubed provides an innovative Software-as-a-Service platform for the monitoring and protection of small and mid-sized business networks based on a small, simple configuration change, with no hardware or software to install. This service provides fresh visibility into business networks at a speed and scale that is unrivaled in the cyber security industry. This report is based on the collection of data from globally-deployed firewalls protecting MSP networks. The purpose of this analysis is to provide context into the extent to which these networks are being attacked and what MSPs can do to help protect their customers from a business-ending breach. Dark Cubed analyzes network traffic in real-time and assigns a simple, actionable threat score to every IP address and Domain Name observed on that network based on three categories of analysis: known threat, predictive threat, and community analytics. The scoring framework, as displayed below, assigns a level of threat and a confidence rating to every communication to enable simplified and automated response activities.

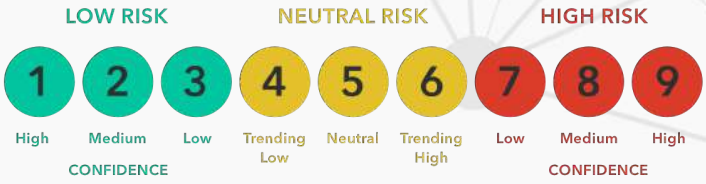


Figure 1: The Dark Cubed Threat Scoring Framework

This scoring approach simplifies expert assessments on cyber security threats to enable businesses to take rapid action on threats to their network without requiring extensive additional analytics or the staffing of additional analysts. The real secret. to cyber security analytics is the ability to automate actions against known and likely attacks to prevent harm, while also enabling business leaders to focus resources on those threats that are most significant. The ability to provide broad-based protection while also maintaining sufficient fidelity is an art form with which even the largest, most well-funded security teams struggle. One key indicator of threat is not the volume, but the rate at which attacks change over time.

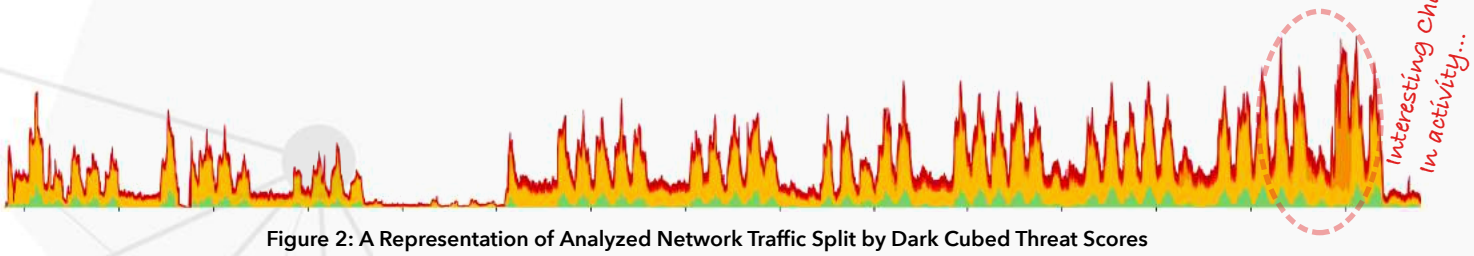


Figure 2: A Representation of Analyzed Network Traffic Split by Dark Cubed Threat Scores

With respect to the rate of change, the figure above represents the volume of traffic across the MSP networks, broken out by the Dark Cubed scoring algorithms. It is clear in this view that network traffic has normal ebbs and flows related to regular periods of business during the week and lags during the weekends. We can also see periodic spikes and lulls in traffic patterns, sometimes related to more active periods of scanning by suspicious or malicious actors. The figure below illustrates the build-up of known and new indicators over the observed period, resulting in nearly a million unique indicators in that period."

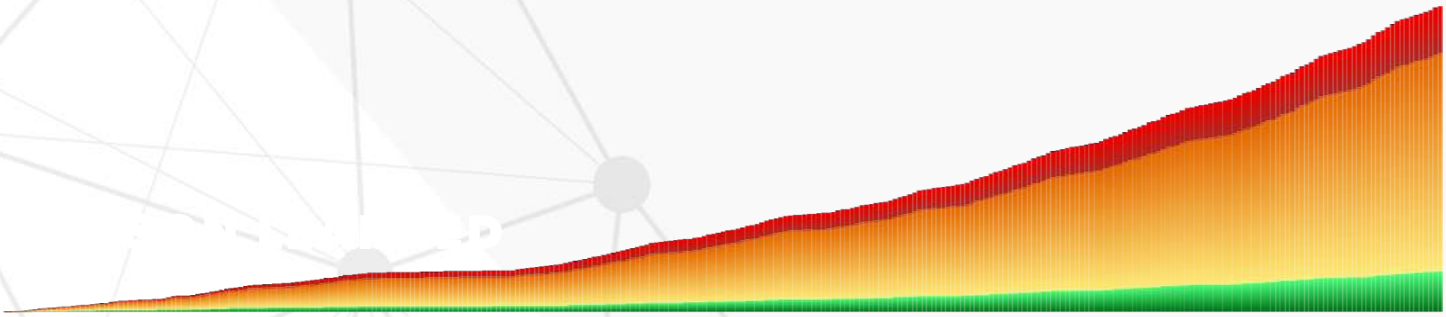


Figure 3: The Buildup of Indicators Over the Analyzed Period

STATE OF THREAT, CONTINUED...

Understanding threat from a high level is an important and a valuable first step, but it is critical to go several steps further to understand the full scope of the MSP challenge. First, to put the types of attack in the context of volume, it is helpful to understand how often those indicators were observed within the data set. As shown below, a majority of the indicators were seen less than 100 times, indicating a relatively low level of commitment to any specific network by the attacker. As we move to the right, we see that less than 800 indicators were seen more than 1,000 times. This group represents two possibilities (A) noisy actors that do not care about being observed or (B) focused attacks utilizing brute-force techniques on one or more networks.

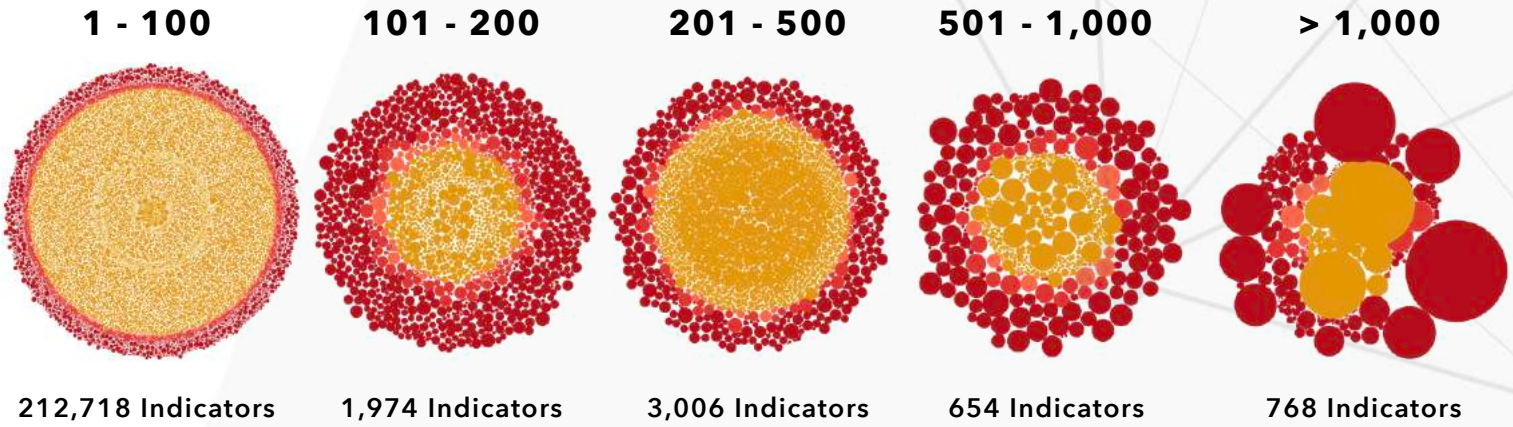


Figure 4: High Threat Indicators Grouped by the Count of Times Seen On MSP Networks

Another fascinating view comes from a look at the first seen and last seen dates for each indicator across the data set and by sizing the day by the count of items last seen on that day. As shown in the figure below, we can see the volume of activity related to threats that were first seen on specific days and their continued activity throughout the time period of the assessment. Two things are clear from this visualization. First, indicators are typically most active when they first show up on a network and perform an assessment of the target network.

Second, after an indicator is observed on a network, it typically does not go away; rather, there is a lingering footprint on the target network to detect changes that could result in a new weakness or vulnerability.

In summary, this data set makes it clear that MSP networks are under a constant state of threat and active attack. While the fact that MSP networks are being targeted may not be a surprise, it is informative to see the extent to which they are targeted by persistent malicious and suspicious threat actors.

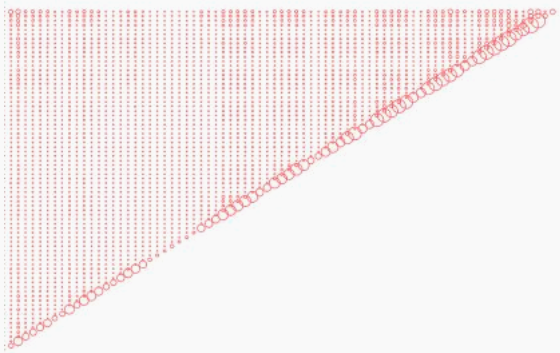


Figure 5: Persistence of Threat Activity Over The Evaluated Period

LESSON LEARNED

Regardless of what is being sold in cyber security advertising, it is clear that protecting a network is much more complicated than simply deploying a firewall with "Advanced Threat Protection." True protection requires data analytics and visibility at a scale that has not traditionally been available to small and mid-sized companies. Any company that has invested significant amounts of money into a cyber security infrastructure will emphatically agree that a firewall is only part of the solution and not THE solution given the current threat landscape.

BOTNET BARRAGE

THE STARK REALITY OF BOTNETS

One of the most striking images to come from our analysis was the relationship graph for botnet activity attributed to the Mirai Botnet across the MSP networks. The resulting graph has over 100,000 nodes and came out looking like an angry sun. To get a better view of the data, we continued the analysis by looking at a single MSP firewall to understand how heavily the Mirai botnet was attacking that firewall.

Figure 6: All Activity by the Mirai Botnet against MSPs

The results were surprising. As shown in the second image below, this single network was attacked by nearly 20,000 unique IP addresses, representing 149 individual countries and 3,607 different organizations.

Top 20 Sources of Mirai Attacks on a Single MSP Firewall

Chunghwa Telecom Co. Ltd.	Taiwan	2800
CHINA169-BACKBONE CHINA UNICOM China169 Backbone	China	1570
Chinanet JS	China	361
Kornet	South Korea	305
Turk Telekomunikasyon A.S	Turkey	263
CHINANET-BACKBONE No.31Jin-rong Street	China	242
Dynamic distribution IPs for broadband services	Russia	242
TE-AS TE-AS	Egypt	215
Vietnam Posts and Telecommunications Group	Vietnam	213
Hong Kong Telecommunications (HKT) Limited	Hong Kong	190
FPT Telecom Company	Vietnam	175
TELKOMNET-AS-AP PT Telekomunikasi Indonesia	Indonesia	144
Telecom Argentina S.A	Argentina	140
Viettel Corporation	Vietnam	139
Charter Communications	United States	137
TTNET	Turkey	134
VIETEL-AS-AP Viettel Group	Vietnam	120
China Mobile	China	119
Chinanet GD	China	116
Global Village Telecom	Brazil	107

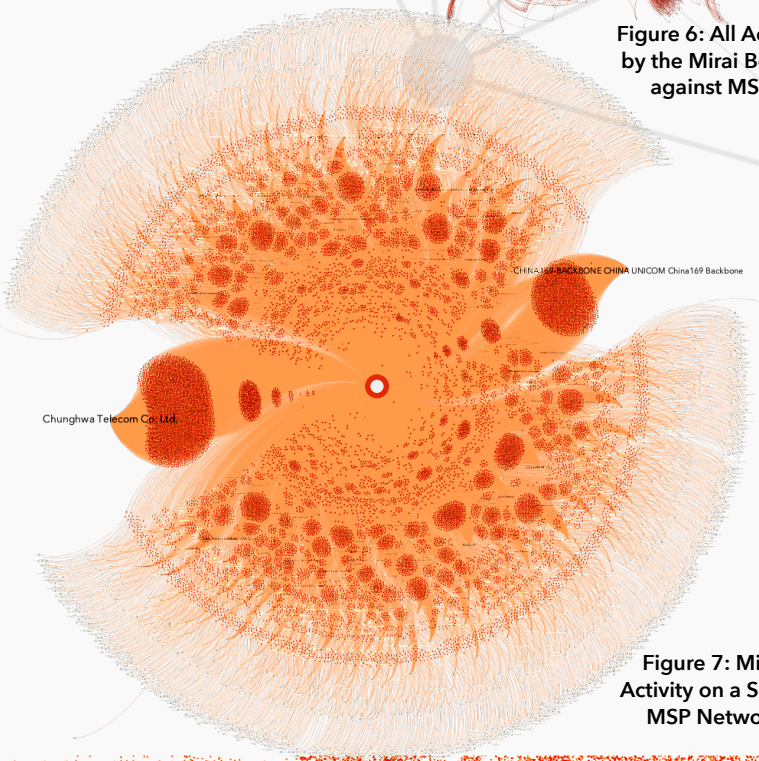


Figure 7: Mirai Activity on a Single MSP Network

As shown in the table above, the top 20 organizations represent a fascinating cast of characters with 2,800 of the IPs coming from a single organization in Taiwan: Chunghwa Telecom. We can attribute another 1,570 IPs to China Unicom's network. Both organizations are clearly illustrated by the clumping in the graph to the right. The final chart shows us each of the attacking IP addresses on their own horizontal line and their activity over the analyzed period of time. We can see the banding of activity as the botnet ebbs and flows over time. Most importantly, though, we can see that this is an ongoing barrage against this MSP network and not just a one-time attack.

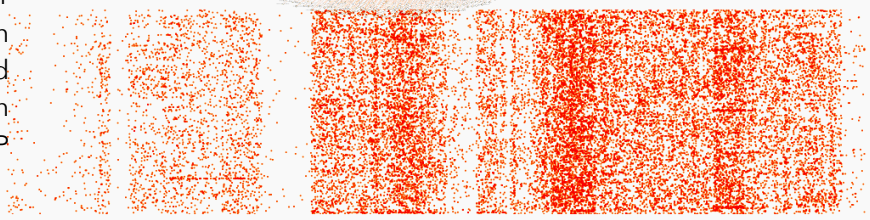


Figure 8: Persistence of Individual Mirai Botnet IPs Against an MSP

LESSON LEARNED

We often hear about MSP networks being targeted, hacked, and having Ransomware distributed amongst their customers. However, once you understand the volume and intensity of this targeting, it becomes clear that one mistake, one misconfiguration, could be fatal. MSPs must improve their network monitoring capabilities and secure their systems against the full-scale attacks they are facing on a daily basis. Leaving common ports open and exposed with weak authentication will absolutely result in a breach.

REMOTE ATTACK

REMOTE ACCESS IS BEING ACTIVELY TARGETED

One of the most common methods of distributing ransomware is related to a threat actor compromising remote access tools such as RMM tools, or Windows Remote Desktop, that utilize weak credentials and do not employ two-factor authentication. A great example of this shows up in our set when we look at traffic associated with port 3389, which is commonly used for Windows Remote Desktop. As you can see by the chart to the right, there is significant activity related to this port across the MSPs we evaluated, as expected. However, what is interesting about this graph is that we can see the big spikes of "legitimate" port 3389 activity that is scored in the low threat range by our scoring algorithms, represented by the yellow-colored mountains. This is a valid and expected remote access activity occurring.

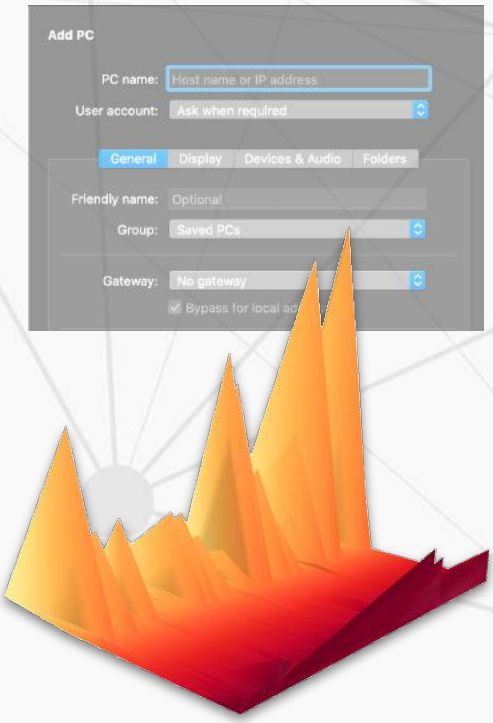


Figure 9: Visualization of Port 3389 Traffic

What is interesting though, is the lack of activity between the range of 6, 7, and 8, meaning our range of "less confidence" for bad activity, before seeing a spike again in activity scored as a 9, or high threat-high confidence. This shows that for this data set, most scanning and probes for remote desktop vulnerabilities are coming from well-known bad hosts.

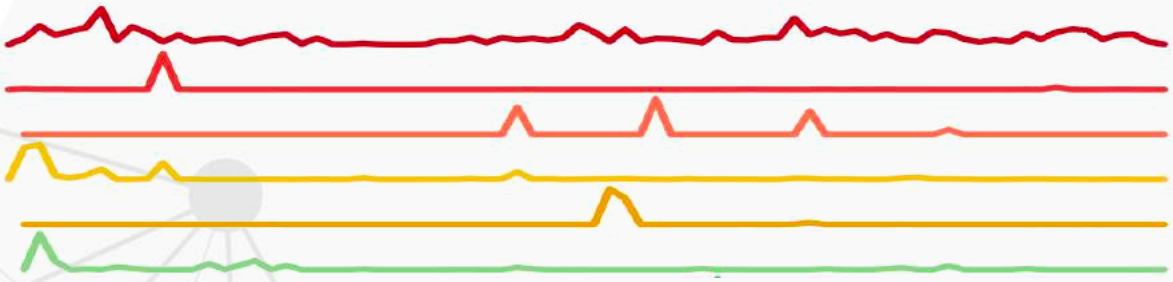


Figure 10: 3389 Traffic Over Time Broken out by Dark Cubed Threat Scores

A different perspective on this same data can be given by looking at activity across threat score ranges split apart by scores. Here we can see the spikes of activity throughout the time period when normal RDP activity occurred at the lower score ranges. We also see a few spikes in the medium score ranges related to one-off activities. However, a majority of the bad activity is related to known-bad IP addresses at the top in the dark red. Here we can see the impact of constant scanning for remote desktop vulnerabilities by malicious actors.

LESSON LEARNED

Remote access tools present the greatest risk to a network due to the number of vulnerabilities associated with this functionality. It is strongly recommended that all organizations put any remote access tools behind a secure VPN with two-factor authentication. If your RMM provider does not offer two-factor authentication, then we strongly recommend you move to one that does. If you expose your remote access capabilities broadly without protection, you will be breached.

FRIENDLY FIRE

THE IMPACT OF "NON-MALICIOUS" ACTIVITIES ON NETWORKS

One of the most significant challenges for any security analyst is related to the volume of alerts that an organization receives from its security infrastructure and the extent to which an analyst can convert those alerts into actionable intelligence. In a recent Poneman Study [1], it was found that 69% of analysts considered having "too many alerts to chase" as one of the most painful parts of working in a security operations center (SOC). Our analysis provided us with a distinctive view into some of the details behind the generation of noise for networks, specifically, the scanning of networks by "good" actors as opposed to malicious ones. For this portion of our research, we turn to our partnership with GreyNoise. GreyNoise provides a unique service in the threat intelligence world of identifying the "background chatter" of the internet through a globally deployed sensor grid that is specifically built for their task. At Dark Cubed, we integrate GreyNoise data into our scoring to enable better decision making and automation on behalf of our customers.

Within our data set, there were approximately 3,500 IP addresses that GreyNoise labels as benign. Those IP addresses were located in 21 unique countries, represented 83 unique organizations, and accounted for around 200,000 scans over the 90 days. This activity was not evenly distributed, but significant as represented in the chart below.

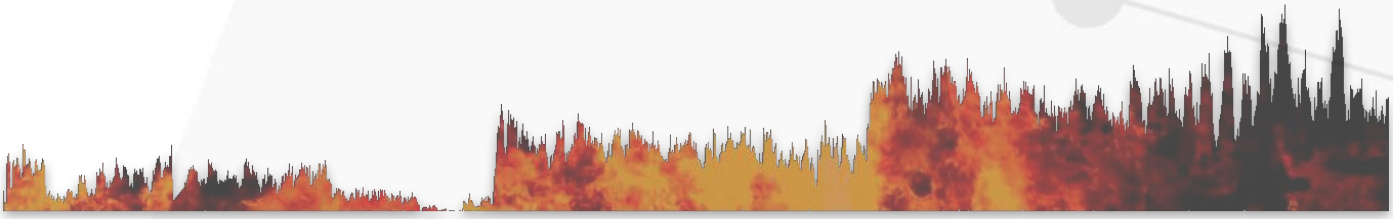


Figure 11: Representation of "Friendly Fire" Data Volume Over Time

It is commonly believed that scanning activities by organizations such as Shodan.io, Censys, Rapid7, BitSight, and others may not be of any harm or cause any concern, but going back to our discussion on the fatigue felt within SOCs by security analysts, it is critical to understand how these go from seemingly harmless scanning activities to analyst overload.

When we compare the 3,411 unique IP addresses with a number of the more popular threat intelligence lists available, the problem quickly becomes apparent. Over 81% of those "benign" IP addresses are showing up on one or more lists, with 2,300 of those showing up on more than one list! This means that if you are using these sources of data as intelligence to guide your analysts, you are killing them with noise.

When we look at those IPs that show up on the most lists, we get a pretty interesting view into those "benign" scanners who are likely scanning at incredibly high volumes across the Internet. The table to the right shows the top 20 IP addresses ordered by the number of threat intelligence lists that show them as a threat. We can see the key actors here are Shodan, Bit Sight, and Security Scorecard. All of these organizations advertise having visibility into networks, and now we know how they get that visibility: massive amounts of scanning.

Most Reported Benign IPs

66.240.192.138	Shodan.io	10
82.221.105.7	Shodan.io	9
82.221.105.6	Shodan.io	9
66.240.236.119	Shodan.io	9
107.6.183.226	Bitsight	8
107.6.183.162	Bitsight	8
198.143.155.138	Bitsight	8
184.154.47.2	Bitsight	8
198.20.70.114	Shodan.io	8
71.6.165.200	Shodan.io	8
71.6.135.131	Shodan.io	8
69.175.97.170	Bitsight	8
107.6.169.250	Bitsight	8
107.6.171.130	Bitsight	8
96.127.158.234	Bitsight	8
89.248.167.131	Shodan.io	8
89.248.174.3	CriminalIP	8
198.20.103.242	Bitsight	8
208.100.26.233	Security Scorecard	8
198.143.158.82	Bitsight	8

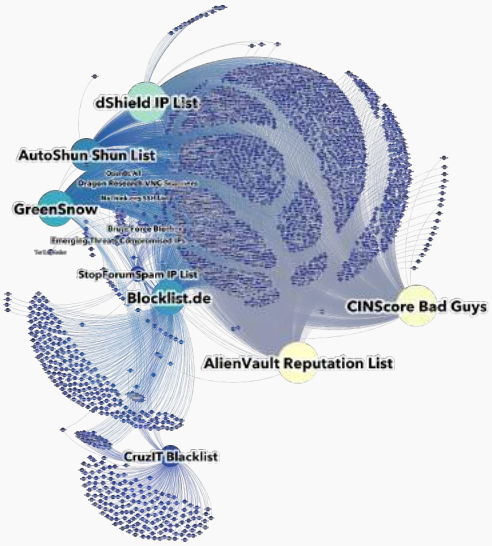


Figure 12: Relationship between "Friendly Fire" IPs and Commonly Utilized Threat Intelligence Feeds

[1] https://www.devo.com/resources/ponemon-soc-effectiveness-report-2019/

FRIENDLY FIRE, CONTINUED...

With the basics on the benign scanners out of the way, the more interesting question regards what this activity looks like across global MSP networks over the 90 days of observation. The volume of data is a bit complex and is difficult to display in a way that makes it easy to digest. The first step is to understand how many unique firewalls actually observed traffic from each scanning organization, giving us a view of how widespread their scanning activities are.

Starting with the upper left, we can see Arbor Observatory hit over 66% of the monitored nodes. Arbor Observatory is related to the company NETSCOUT, who sells a range of services, to include threat intelligence based on the data gleaned in part from their scanning activities. We can also see top placement from the nonprofit Shadowserver Foundation and BitSight, a company that attempts to grade companies based on a number of factors, to include their footprint on the Internet. When we pull this activity out across all of these networks, it provides us with fascinating insights into the scanning methodologies utilized by these organizations.

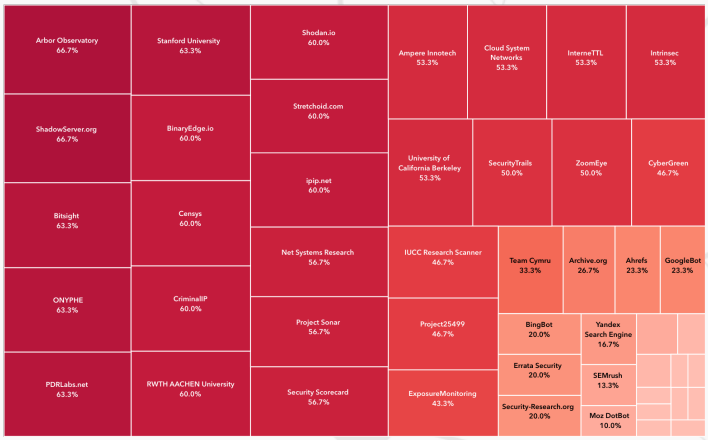


Figure 13: Percent of Networks Targeted by Scanning Organization

To view this activity from a different perspective, we can look at the patterns of scanning associated with each of these services to get a better feel for how their scanning activities are organized. The graph below, while consolidating an incredible amount of data, is interesting, as it reveals these activities. The chart is organized by placing each scanning IP on its own horizontal line, sorted by scanning organization. We can see the groupings created by the different scanning patterns of each service. The dots are then further colored by the firewall that observed the scanning activity. In one example, we can see, as indicated by the blue bar, one organization that got scanned by many of the organizations in a relatively compressed time period.

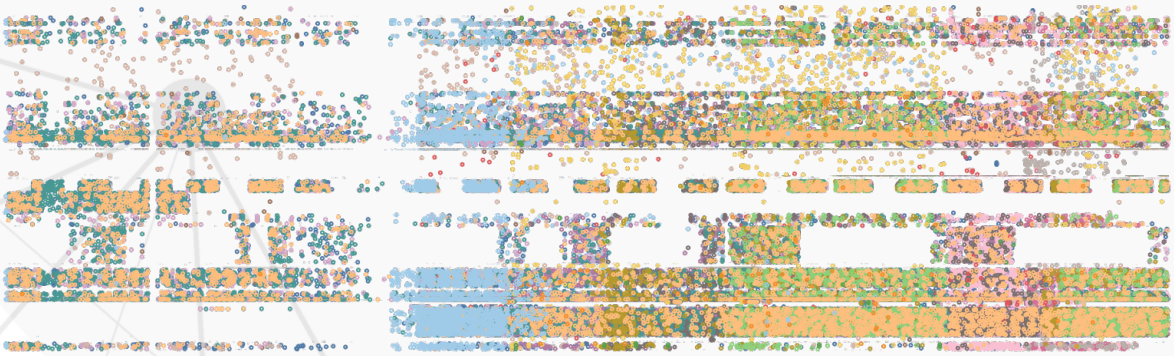


Figure 14: Visualization of Scanning Activities Across All Organizations

To be clear, we are not saying that the scanning activities performed by the companies are wrong. What we are saying is that there is a strong overlap of automated threat reporting and threat intelligence services with the infrastructure used for this scanning, resulting in an overwhelming amount of noise that potentially enables malicious threat actors to slip through the door while the defenders are chasing their tails.

LESSON LEARNED

The security community needs to develop an approach to differentiate between beneficial and malicious scanning activities in a fully automated, orchestrated approach. Without taking action, network defenders will become increasingly buried in noisy network activity that will prevent them from being able to identify real attackers at the most critical times.

DEADLY SONAR

YOUR NETWORK IS UNDER CONSTANT SURVEILLANCE

Botnet-related activity was covered in a previous section, but now we will take look at scanning activity by other malicious actors to see what we can learn. A threat actor can use Nmap to scan all of the ports on a system to see which ones are open, or they can scan a broad swath of the Internet to look for specific open ports using a tool such as Masscan. Both of these tools are freely available and can be up and running on a new server within minutes. While many of these activities could still qualify as noise due to their broad targeting, they represent an actual enemy performing reconnaissance on a real target. The chart below shows the activity of nearly 64,000 IP addresses that were identified by our analytics as scanners targeting these networks. This chart is colored by scanning host and sorted by ports, with the lowest ports being at the top and the highest ports at the bottom.

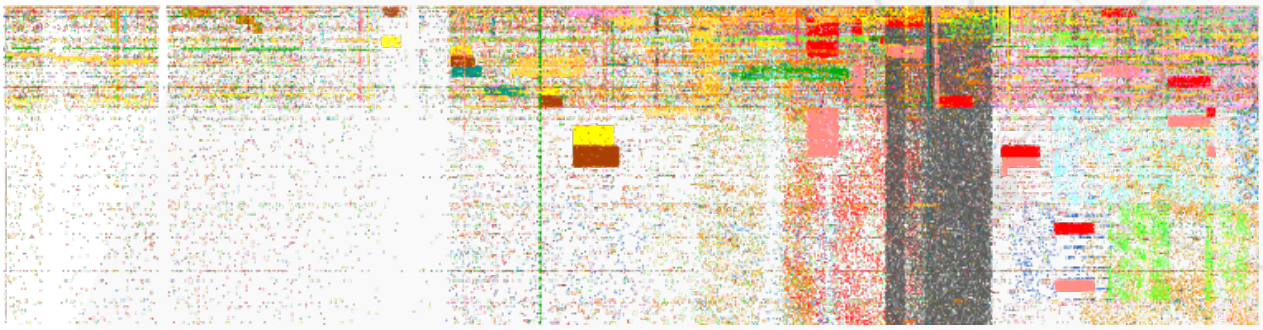


Figure 15: Malicious Port Scanning Activity Across All MSP Networks

Gaining the macro view of these activities is incredibly valuable to understand how attackers are targeting networks. We can see the level at which these threat actors are targeting these firewalls every single minute of every single day. For example, in the figure below we see a very large, gray vertical bar, which represents a single host using a Digital Ocean server in the Netherlands to hammer against a single MSP firewall across all known ports over seven days. What is perhaps even more intriguing about this endpoint is that the actor was focused on a single target network and likely used this server for a limited period of time before moving servers to avoid detection.

One critical component to understanding such activities comes from determining if the scanning activity is broad and your network is just collateral damage or if your network is the actual target. Remember how we discussed that Digital Ocean host above? If we regenerate the above chart, but only show those hosts where GreyNoise has not seen the hosts conducting broad scanning, the results are stark. This ability to separate signal from noise at scale and enable automation is a key to helping small and midsized companies gain the upper hand in the fight for digital security.

Figure 16: Malicious Port Scanning Activity Across All MSP Networks With the "Noise", or Broad Scanning Hosts, Removed

LESSON LEARNED

The amount of time between an exploit or vulnerability being released into the wild and broad scanning for systems susceptible to attacks is increasingly small. If networks are not properly locked down and patches are not quickly applied, the likelihood of a breach is almost guaranteed.

DIGITAL SHARKS

A VIEW OF TRAFFIC COMING FROM DIGITAL OCEAN SERVERS

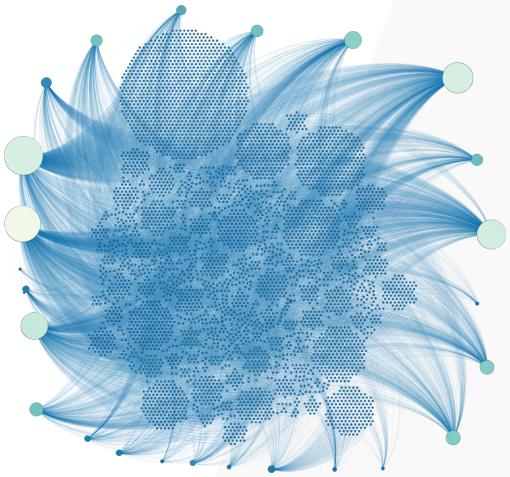


Figure 17: Visualization of Communications with Digital Ocean Hosts

Cloud infrastructures have been an exciting development in the IT community over the past decade, resulting in a rapid proliferation of online providers ready to get you into a new, shiny server in a matter of minutes. One of the things we consistently see in our customer base, and it is apparent in this data set as well, is the prominent role that the cloud providers play in the threat landscape. The graph to the left shows a number of MSP firewalls on the outside, and the 5,093 Digital Ocean-hosted servers that we observed communicating with those firewalls. At first glance, this is a pretty exciting view if you are Digital Ocean. Digital Ocean servers appear to be heavily used for a wide variety of purposes. However, when we overlay a filter of IP addresses that have been flagged for malicious or suspicious activity, things change quickly.

On the right, we can see the same graph with those IP addresses identified as high threats by our scoring algorithm highlighted in red. This is a pretty impressive view of the extent to which Digital Ocean is used for negative ends. This revelation that Digital Ocean environments are being used for malicious activity is of significant concern to MSPs, as 31% of the Digital Ocean IPs observed in the dataset are likely being used for nefarious purposes.

31% of the observed hosts related to Digital Ocean were identified as performing suspicious or malicious activities.

There are two serious outcomes from this analysis of Digital Ocean traffic. 1) Attackers are able to rapidly establish an environment, execute attacks, and then shut down faster than defenders can respond with traditional approaches. 2) Whoever inherits that IP address after the attacker has used it is likely to end up on a number of "black lists," requiring days and weeks of effort to rehabilitate the IP address "reputation."

Our findings bring up an important question: With companies like Digital Ocean, to what extent are they or should they be policing their users to limit suspicious or malicious activities? Regardless, it is clear from our analytics that companies should be suspicious about traffic coming from sources like Digital Ocean for the time being.

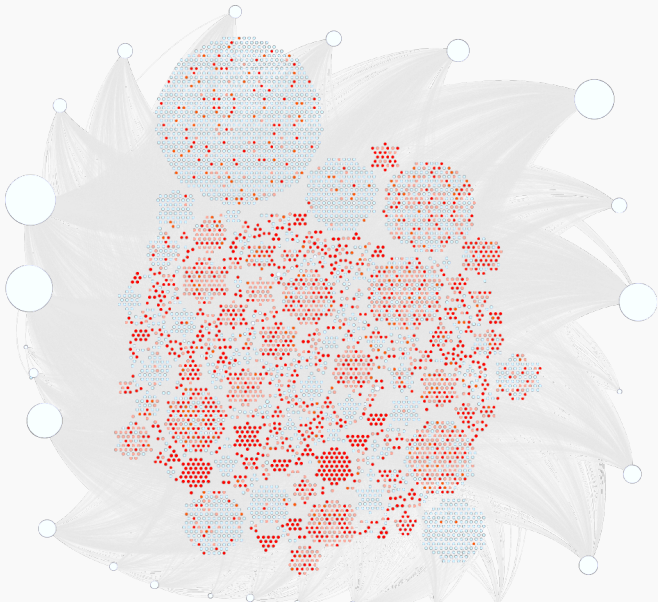


Figure 18: Digital Ocean Visualization with Malicious Hosts Colored Red

LESSON LEARNED

It makes the job of the defender more difficult when attackers can use "ephemeral" infrastructure, such as hosting environments provided by Digital Ocean and others. Such activities require more nimble, flexible security organizations that have the ability to go beyond simply using threat intelligence as a guide due to the long timelines that traditional intelligence takes to produce. Further, organizations must consider implementing the capability to "age out" indicators based on their respective ownership and behaviors.

RECOMMENDATIONS

A FEW COMMON SENSE RECOMMENDATIONS FOR MSPS

This report represents a unique view of the current state of cyber security threats being faced by MSPs on a daily basis. By focusing on real network traffic and documented, repeatable analysis, we have provided one of the starkest views into the level of attack these networks are facing.

The findings of this report make it clear that managed service providers must reorient their business strategies to reflect the fact that they are now operating in an environment where any mistake, any error in a network configuration, is likely to result in a breach. Below are a few recommendations for MSPs to consider when implementing security programs for their networks and the networks of their customers. This list is not intended to be complete, rather as a quick reference guide. For a complete security program, refer to the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST).

- [ ] **Remote Access:** Place all remote access capabilities behind a VPN that utilizes two-factor authentication. If using an RMM tool, require the use of two-factor authentication on all accounts. If the RMM provider doesn't offer two-factor authentication, switch providers.

- [ ] **Password Management:** Organizational password policies should be applied to MSP accounts and customer accounts. These policies include complexity, limiting reuse, lockout, and logging. Educate all users to not utilize the same password across accounts. Consider the use of a password management tool that can be protected with a complex password AND two-factor authentication.

- [ ] **Service Accounts:** Use service accounts for MSP agents and services. If an MSP requires the installation of an agent or other local services, create service accounts for this purpose. Disable interactive logon for these accounts.

- [ ] **Manage Access:** Restrict MSP accounts by time and/or date. Set expiration dates reflecting the end of the contract on accounts used by MSPs when those accounts are created or renewed. If MSP services are only required during business hours, time restrictions should also be enabled and set accordingly. Consider keeping MSP accounts disabled until they are needed and disabling them once the work is completed.

- [ ] **Network Architecture:** Use a network architecture that includes account tiering so that higher-privileged accounts will never have access or be found on lower-privileged layers of the network. This keeps EA and DA level accounts on the higher, more protected tiers of the network. Ensure that EA and DA accounts are removed from local administrator groups on workstations.

- [ ] **Threat Analytics:** Implement a robust threat analytics capability that integrates threat intelligence from multiple sources on the MSP network and the networks of MSP customers to detect changes in the threat environment. Utilize tools such as GreyNoise to reduce analyst fatigue from noisy threats.

- [ ] **Government Reporting:** Monitor reports published by government sources, such as the National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). For example, TA18-276B covers Advanced Persistent Threat Activity Exploiting Managed Service Providers. This report can be found here: https://www.us-cert.gov/ncas/alerts/TA18-276B

THANK YOU!

If you made it all the way to the end and are still reading this, then thank you for your time and support. We know the volume of noise in the cyber security market can be overwhelming, and the fact that you stuck with this report to the end means something!

If you have any feedback, comments, or questions on this report, please let us know by contacting us at info@darkcubed.com.

Follow us on Twitter at @darkcubedcyber to stay up to date on future reports and other cyber security-related updates.

dark3

dark^3