Ransomware

Remote Access and IoT Search Engines

Recently, Arete Incident Response Tiger Teams ("Arete IR") have responded to an increased volume of ransomware incidents involving the Sodinikibi, Phobos, and Dharma ransomware variants. The threat actors deploying these variants are known to use anti-forensics techniques to hide their tracks. Once access is gained, they usually delete artifacts which aid cyber investigators with reconstructing steps taken by the threat actors, revealing important information pertaining to the root cause for the computer security event. In most cases, Arete was able to recover critical artifacts to forensically reconstruct the various attacks to identify a single entry point consistent across the three variants: Remote Desktop.

Requirements

Businesses have a need to enable workers to access files and business resources remotely from home, hotels, or business relationships. The cheapest way for businesses to allow remote access is to "expose" the Remote Desktop Protocol ("RDP") to the public internet. The business' firewall configuration is altered to allow inbound connectivity to the default port 3389, and any connections to that port are automatically forwarded to a specific computer on the network, which is usually a terminal services server. Using only an Internet Protocol ("IP") address, anyone can attempt to connect to the RDP service.

Limitations on Protocol and Service

Most businesses who implement remote access via RDP aren't aware of the limitations of the service nor do they implement intrusion detection and prevention services. Lastly, many don't require multi-factor authentication. The downside to allowing any connection into a network is exactly that: any connection can be allowed into the network. This connection can be from anywhere, at any time, for any reason and with any number of authentication attempts. The RDP service itself doesn't monitor for bad credential combinations and automatically disable or block connection attempts. Port forwarding on firewalls doesn't inspect the inbound traffic either. Essentially, once a port is exposed to the public internet, anyone, anywhere, can try an unlimited number of usernames and passwords to gain access to that system. Since any number of combinations can be attempted, this makes the configuration vulnerable to credential stuffing, dictionary, and brute force attacks.

Crime of Opportunity

Quite often during our investigations, clients ask "was this a targeted attack or a crime of opportunity?" Nine out of 10 times, it's a crime of opportunity. Then the follow up question "Why us?" Well, for starters, it's your configuration. These threat actors have their attack mechanics down to a series of steps:

1. Identify target
2. Gain access to target
3. Cover tracks
4. Deploy ransomware
5. Repeat

While they most likely aren't outright targeting your organization directly, they may be targeting exposed services which link them to your organization.

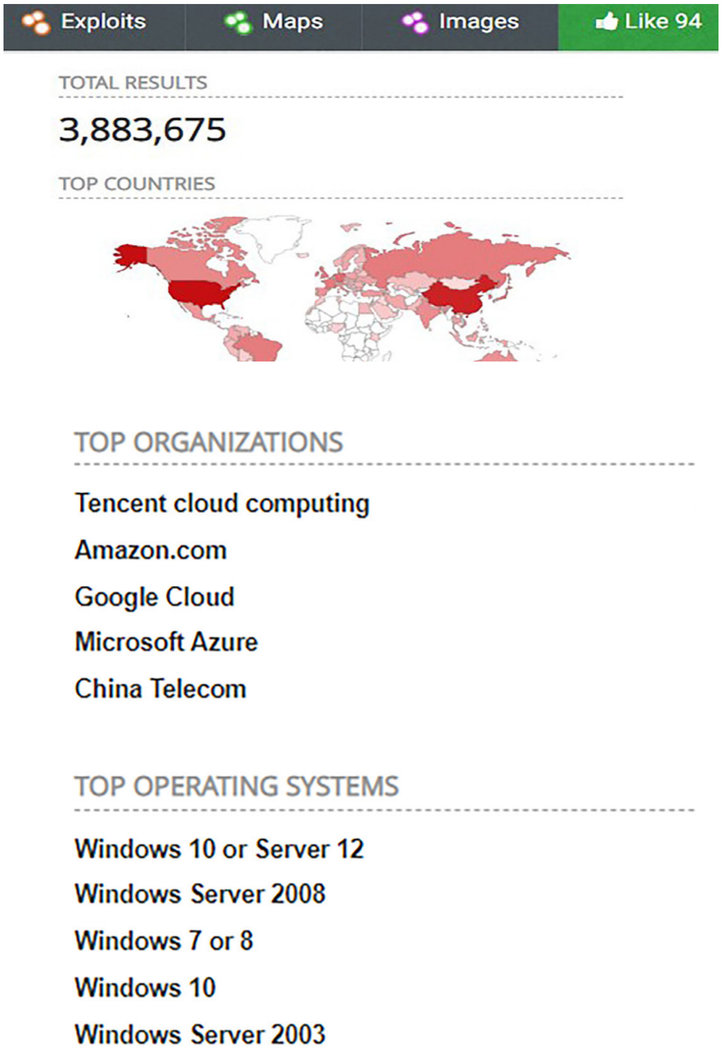
Internet of Things (IoT) Search Engines

Google, Bing, and DuckDuckGo are three very popular search engines. They're used to find all sorts of text information or images. These search engines aren't designed to identify specific computers or services across the world. Rather a different set of search engines can be used to find computers that are connected directly to the internet along with their IP addresses and any other information about the computer involving their geo location, running services, and protocol history. Use caution when visiting these sites as unintended side effects can occur.

1. https://shodan.io
2. https://censys.io
3. https://zoomeye.org

These sites can be used by anyone, anonymously, to identify internet attached devices, the services they're running and any other information the IoT crawlers can index. The anonymous feature is obtained via the IoT indexer by allowing anyone to query the index stored by the IoT search engine, instead of scanning the node directly. Essentially, this search engine is the phone book, allowing anyone to find street addresses by person's names or people by street addresses.

A search for "port:3389", which is the default port for RDP services, can return several million devices. Again, this isn't real time information because the query is run against the index of the IoT search engine. Once an IP address is identified, additional steps would be needed to test if the IP address is online. Additionally, the resulting information can be filtered by organization, operating system, and country.



TOTAL RESULTS

3,883,675

TOP COUNTRIES

TOP ORGANIZATIONS

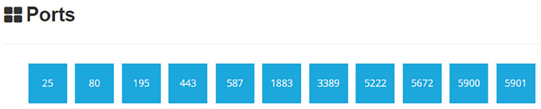
Tencent cloud computing
Amazon.com
Google Cloud
Microsoft Azure
China Telecom

TOP OPERATING SYSTEMS

Windows 10 or Server 12
Windows Server 2008
Windows 7 or 8
Windows 10
Windows Server 2003

Reviewing the results, there's approximately 1,060 IP addresses that are detected as the Windows 2003 operating system. At face value, this is extremely alarming because Windows 2003 was discontinued during July of 2015. Microsoft officially stopped supporting the operating system as well as providing security updates. Given the information returned from shodan.io, businesses are still relying on it as a means for remote connectivity. Again, these results would need to be qualified as online and available. Regardless, the number is still alarming.

Attack Methodologies



Ports

25 80 195 443 587 1883 3389 5222 5672 5900 5901

After the threat actor identifies a target, any number of steps can be performed to initiate an attack. Typically, the threat actor will profile the target to gain as much information as possible in order to increase the success of the attack. Profiling can occur in any of the following ways:

- Verifying the IP address is online and attempting to brute force access automatically.
- Attempting to resolve the IP address to a domain name or company name in order to:
    - Construct phishing emails for obtaining credentials.
    - Employ social engineering of employees for obtaining credentials
- Research running services against known vulnerabilities to identify pre-built payloads to exploit the services.

Whichever approach the threat actor takes, there's a good chance they will be successful with gaining unauthorized access to your network.

Preventative Actions

While it's a waiting game to become the next victim, there are steps you can take to mitigate or prolong falling prey to these threat actor methodologies. Successful mitigation of unauthorized access can be achieved through the proper implementation of layered computer and network security controls. The following steps, while not exhaustive, can be taken to mitigate the exposure of services used by your organization.

- Enable Multi-Factor Authentication ("MFA") on any third party accounts or remote access accounts.
- Disable RDP services and port forwarding on firewalls.
- Implement VPN services to remotely connect to your organization's network or leverage remote connection technologies that support MFA.
- Research open source intelligence to develop a public footprint of your organization.
- Train employees on social engineering and phishing email tactics and techniques.
- Purchase a cyber insurance policy and familiarize yourself with the preferred vendors within your policy.
- Build a close working relationship with a cyber advisory company.