NETFOUNDRY™

SPIN UP YOUR NETWORK

SECURITY PAPER

How Do Ransomware Actors Find Victims?

How do Ransomware actors find victims?

It is obvious from the news these days that the world is faced with a ransomware epidemic. Criminal actors exploit vulnerabilities in networks and applications to extort money from enterprises, end users, and others. The same types of actions can also be leveraged for actual cyber warfare, attacking infrastructure, financial, physical, and digital. For those outside the technical arenas of IT and cybersecurity, it can be difficult to understand how these things happen, and for those in the fields, it can be difficult to explain to management and others how these things happen.

This is the first of three papers in which I will show how ransomware actors seek out potential targets, how once identified attackers gather information about attack vectors into organizations, and in part three discuss steps and strategies you can deploy to thwart and mitigate attack scenarios. All three papers are available from the NetFoundry web site.

We start with an explanation of the path an attacker could take to successfully exploit a network, including references to recent attacks that have used these methods, or likely have. Next, I will show how simple it is for a user to recreate most of the attack path with easily downloadable software and open public systems. Lastly, I will discuss how NetFoundry application embedded security can help to mitigate these attack vectors and secure your users and the enterprise.

Throughout these articles, I will reference the MITRE ATT&CK® framework. MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior. You will see references to {TAXXXX) or (TXXXX), indicating tactic or technique, respectively. These can be used to look for more information in the ATT&CK knowledge base, should you choose. ATT&CK is an extremely valuable resource for the cybersecurity world. If you are a nontechnical reader you may read the references without any further concern. If you would like to understand more about the ATT&CK framework and the information it contains, please use the references to find more information on the topic. If you are an IT

or cybersecurity practitioner and you are not familiar with ATT&CK, I strongly suggest you research it. There is a wealth of resources available at https://attack.mitre.org and ATT&CK is rapidly becoming a central language for breach reporting and understanding.

How Network Scanning Can Discover Vulnerabilities

For the breach described in this paper, we will follow a particular attack path – namely, this breach utilizes network scanning. This is one of the most common pathways that can be leveraged for ransomware and other attacks, phishing being another. We will look at network scanning here as it is far less discussed, but at least as dangerous as phishing.

ATT&CK enumerates a tactic called Reconnaissance as TA0043, a high number, but the far left of the matrix, as it is truly the starting point for cyberattacks. As the name indicates, this phase of an attack is to gather information about potential targets. These targets may be selected for particular reasons such as politics, revenge, gaining "cred" in the cybercriminal world, or others. Or they may be selected purely because they are vulnerable. But how does a cybercriminal actor find the server in your network that is vulnerable given the billions of Internet-connected devices in the world, especially if YOU don't even know it is there? We will discuss two major techniques to discover these potential targets. Later, we will discuss the actual mechanisms and examples of utilizing these practices.

Active Scanning (T1595) describes the steps of using a system and process to find potential targets, or to map out targets with more detail. Actrive scanning has two sub techniques, IP Block Scanning (T1595.001), and Vulnerability Scanning (T1595.002). These processes are very similar. They both use active network traffic to elicit responses from potential targets to identify them. In the case of IP Block Scanning, the scans are meant to look for available systems and services. This is normally done by sending TCP SYN packets (The first packet sent in most Internet conversations) and recording whether or not there was a response, and what the response contains. TCP Ports are usually indicative of particular services. Port 22 is assigned to SSH, Port 80 to HTTP, 443 to HTTPS, and 3389 to RDP. By seeing what ports are available on what nodes, attackers can then make plans for potential attacks.

Vulnerability Scanning (T1595.002) is very similar but more intrusive. Given a set of IP addresses, a vulnerability scanner will execute scripts that are intended to show whether the system has a particular flaw. It may be a configuration option that allows anonymous access, an injection vulnerability, or something else. The reports of these scans enumerate all the potential vulnerabilities discovered. This gives more detailed information about potential attack vectors and this information can be used very effectively in automated attacks, exploiting the weakness to install a Remote Access Trojan (RAT) or other malicious software the attacker can come back to later to exploit. Custom-made vulnerability scanning is often created around recent public reports of weaknesses or zero-day vulnerabilities. These issues often create a race between attackers and defenders (IT and cybersecurity teams) to exploit a weakness vs. remove or mitigate it.

Both techniques can also be used as valuable network management and security tools. Performing these kinds of checks against your own infrastructure should absolutely be done regularly so that issues can be found and patched before "the bad guys" take advantage of them. In the malicious actors' hands, these techniques are just as powerful. The selection of these techniques' use can be dependent on a number of things.

IP Block Scanning is a lot easier to "hide", pacing the requests, obfuscating them with similar requests from spoofed addresses (fictitious systems), etc. Vulnerability scanning with a general use scanner is very easy to find and will often set off alerts and events that IT and security teams can investigate. Vulnerability scanning is rarely used by more advanced actors, but is very easy to do, and can be quite effective. If you don't think your systems are being probed by these techniques, I can assure you, you are incorrect for Internet addressable hosts. A system with nothing running on it sitting in a cloud can receive packets from thousands of systems per day. Any services (ports) found will be probed for default credentials, etc. immediately. All of this activity is automated, simply scanning the Internet 24 hours per day, every day, looking for easy pickings.

Publicly Available Scanning Tools

Some of these scanners operate for research and semi-commercial reasons, without being criminal in any way. Shodan is perhaps the best known example. These systems scan the

Internet constantly, and make their findings known. You can search their databases for several things, domain name, IP address, port number, even SSL certificate information. This can be very useful for several reasons, like most things, to both attackers and defenders of information resources. Searching these types of resources is another ATT&CK enumerated technique, Search Open Technical Databases (T1596), particularly Scan Databases (T1596.005). This allows malicious actors to pull information without operating their own scanners, and possibly giving away their location. As far as the attacker is concerned, the checks are completely passive, since Shodan or other services have already done them. Reputable systems, like Shodan, will give information so that users can "hide" their systems via network or node security configuration. They post the scanning source IP ranges, etc. This makes the data somewhat less useful to potential attackers, but it is still a strong information resource.

Exploiting User Identities and Credentials

Once potential targets have been discovered from the sea of nodes connected to the Internet, exploitation can begin. In most cases, especially ransomware attacks, user identities are required. These credentials will be used to gain access to the information resources to be exfiltrated or encrypted in place. This moves us along the ATT&CK matrix to Initial Access (TA0001) and Credential Access (TA0006) techniques. The combination of techniques within these tactics can give attackers all the access they need to your networks and resources.

Initial access often begins with either Exploit Public-Facing Application (T1190) or External Remote Services (T1133). Public-facing applications may be deployed for several reasons such as providing a service, lack of security controls and understanding, or to enable access from remote users, etc. Some of these use cases are normal and are fine if secured properly. If not secured properly, these situations can lead to significant impacts.

The Kaseya ransomware attacks are examples of this sort of application becoming an attack vector, the Salt crypto mining events are another. In both events, a vulnerability was discovered and using some of the scanning techniques above, targets were located and exploited very quickly. The details of Kaseya are still vague, and thus far it is not currently indicated to be a credential-based attack but is a strong example of the dangers of placing

applications in a position of being directly accessible from the Internet. External remote services are often SSH, SCP, RDP, VPNs or other services used to provide users access to enterprise resources remotely. These services often run on well-known ports and are easily identifiable with scanning or scan database results.

How are these externally reachable services exploited? Some exploits take advantage of issues within the software, allowing it to be manipulated to allow access by outside actors (people not authorized to access the service). Often, Valid Accounts (T1078) are used by bad actors. These may be default credentials, as implicated in the Mirai botnet attacks a few years ago, or more recently, valid user accounts for the ransomware attack on the Colonial Pipeline. There are a large number of ways to improve identity and access management. Examples include making sure you have clean processes, multifactor authentication, and others. I won't discuss these here but will point out that while these mitigations are well known, and have been for decades, they are often not done, or not done well, resulting in many breaches report weekly. In the case of the Colonial Pipeline, it seems the user may have reused a password from another site, allowing the attacker to "guess" the password relatively easily, having a restricted set of passwords to try. Credential Access (TA0006) is a big business in the criminal side of the Internet. Breached user data is collected, curated, and offered for sale on the dark web. This data is used for these types of attacks and continues to be useful to criminal actors. Selling user data is big business as indicated by the prices it demands, and the increasing sophistication of the data being made available.

Making the connection between user names and potential targets is relatively simple and automatable as well. Steps to Gather Victim Identity Information can utilize social media sites like LinkedIn, company "Meet the Team" pages or many other public sources of information to winnow down the millions of potentials to just a few username/password combinations to try. Once the actor has a foothold in a system, they may act quickly to monetize the access, or may simply drop off some access software (aka a back door) to enable easy access at a later point, when they have more time, or when "the heat is off", and defenders aren't looking quite so specifically at the vulnerabilities they are using to exploit the system.

I am very against using Fear, Uncertainty, and Doubt (FUD) in cybersecurity discussions. Playing "what if" games about unlikely scenarios to shock management, customers, or others is often counterproductive. However, what is described above is a collection of tactics and techniques that is being performed every single day, against many Internet-facing nodes. You don't have to have enemies, you don't have to be a government agency, or a bank, or Fortune 500 company. The automation and ease of monetization means your systems are under constant assault. You must take at least some basic actions to defend yourself if you intend to remain in business and not experience significant losses.

The US Cybersecurity & Infrastructure Security Agency (CISA) provides some great resources to understand basic cyber hygiene practices, regardless of the size of your organization. To understand some of the ways you can emulate attackers with common downloadable software, and pro-actively check your own security posture for the risks discussed here, please follow on to part 2 of this series. If you want to skip straight ahead to part 3, where I will discuss how NetFoundry can assist in mitigating some of the risks. All three of these papers can be found freely available on Netfoundry.io in the "Resources" section.

Learn more with these resources:

All Papers in this series are posted here:

https://netfoundry.io/resources/#whitepapers

Web: https://netfoundry.io

Blog: https://netfoundry.io/about/blog/

Connect on Social Media:

Twitter: @NetFoundry
LinkedIn: https://www.linkedin.com/company/17955047

About The Author

Mike Gorman, Head of Security and Compliance, NetFoundry

Mike is a seasoned Network and Security Engineer and applies his decades of experience as the Head of Security and Compliance for NetFoundry. Mike designs and manages NetFoundry's Security and Compliance program (including SOC-2 reporting) to ensure NetFoundry operations and products are secured properly, while helping to maintain an agile and highly automated development processes. In addition, Mike is a senior member of NetFoundry's engineering team, and in this role has developed monitoring and measuring systems, cloud deployment automation and DevOps tooling. Prior to NetFoundry Mike held a variety of Security and Solution Engineering roles with IBM, and Verizon.

About NetFoundry

NetFoundry is the leader in Cloud Native Networking, enabling businesses to simply, securely and cost effectively connect distributed applications across edges, clouds and service meshes.

The NetFoundry platform, delivered as NaaS, enables businesses to connect applications without the costs and complexity of VPNs, custom hardware, and private circuits. NetFoundry's platform is accessed via APIs, SDKs, and DevOps tools integrations, enabling practitioners, application developers, and network administrators to get the levels of automation and agility which are only possible with connectivity-as-code.

*Disclaimer:

The information provided in this paper is offered "as-is", and is provided for general information purposes only. All information is provided in good faith. We make no representation or warranty of any kind, expressed, or implied in any way regarding the accuracy, adequacy, validity, availability or completeness of any information contained in the paper.