VECTRA
Security that thinks®

2019 Spotlight Report

An inside look at RDP cyberattacker behaviors and targeted industries

VECTRA
Security that thinks®

TABLE OF CONTENTS

Cyberattackers follow the path of least resistance to achieve their objectives. They will attempt to use existing administrative tools before they use malicious software to perform internal reconnaissance, move laterally or exfiltrate data from a network.

One of the most popular administrative tools is the Remote Desktop Protocol (RDP). RDP has become a requisite tool for system administrators because it allows them to control remote systems with the same functionality as if they were accessing it locally. It is even more vital for managed service providers that use it to access hundreds of client networks and systems from a centralized operations center.

In September 2018, the FBI warned that the malicious use of RDP "has been on the rise since mid-late 2016." The FBI also reported that several high-profile ransomware attacks, such as Samsam and CrySiS, utilized RDP to laterally move inside of networks.

Data from Vectra® confirms that RDP remains a popular technique for cyberattackers, with 90% of the organizations in which the Cognito® platform is deployed exhibiting some form of RDP cyberattacker behaviors from January-June 2019.

In August 2019, Microsoft announced four new critical RDP vulnerabilities, all of which are "pre-authentication," meaning they can be executed without proper credentials or input from the victim. Strikingly, these exploits worked for Windows 7, 8, and 10. As Windows 10 is currently the latest and most popular Windows operating system, this suggests that RDP attacks will persist, even as organizations update their IT systems.

RDP gives an attacker direct access to a system, and when that system uses unsecure passwords and default settings, disaster ensues. Even worse, attackers can disable endpoint protection, thereby circumventing critical security controls as they establish a foothold in the organization. Once this happens, prevention tools are blind to the actions of the cyberattacker.

There is risk when RDP systems are internet-facing because they can enable a cyberattacker to easily gain access to an organization's network. Once the bad actor gets in, RDP becomes an even more useful tool.

As attacks progress across the attack lifecycle, cybercriminals can use RDP to perform reconnaissance and lateral movement as they look to identify systems containing valuable data and gain access to them. The ubiquity of RDP on Windows systems and its regular use by system administrators makes RDP the perfect tool for cyberattackers to avoid detection.

Because these types of attacks will continue to be a risk in the foreseeable future, it is important for cybersecurity professionals to develop an understanding of how cyberattackers use RDP. Proprietary detection data from Vectra sheds some light on the distribution of RDP attacks across industries and organization sizes.

Data

The Cognito platform from Vectra includes two RDP detections. The first, RDP Recon, is triggered when a host repeatedly attempts and fails to establish an RDP connection to a workload or a host. This can occur when a cyberattacker tries to determine the active accounts on a system or attempts numerous account logins with common or default passwords in a password spraying attack.

The second RDP detection, Suspicious Remote Desktop, is triggered when a host successfully initializes an RDP connection to another host or workload, but with unusual characteristics. For example, when a computer with a French character keyboard connects to an RDP server that normally receives English keyboard inputs, the Cognito platform will flag it as Suspicious Remote Desktop.

Cognito analyzes all network traffic to learn the normal behavior for each host or workload running RDP. Keyboard language is one of many attributes that is learned in order to indicate RDP misuse.

By analyzing data in the 2019 Black Hat Edition of the Attacker Behavior Industry Report from Vectra, trends in RDP detections from January-June 2019 have been identified.

RDP used in real-world cyberattacks:

APT39 – Cyber-espionage group in Iran focused on personal information

Identified by FireEye in January 2019, an Iran-linked cyber-espionage group tracked as APT39 is carrying out a widespread campaign using a broad range of custom and off-the-shelf tools.

APT39 focuses on personal information to support monitoring, tracking and surveillance operations that serve Iran's national priorities, and to create additional accesses and vectors to facilitate future campaigns.

Operating since 2014, APT39 focuses its operations in the Middle East. Other entities targeted by the group exist in the United States, Europe and South Korea. Most victims belong to the telecommunications and travel industries, but the high-tech industry and government have also been targeted.

APT39 facilitates lateral movement through RDP and other administrative tools. In addition to using RDP for lateral movement, APT39 has used this protocol to maintain persistence in the victim's environment.

Earlier state-sponsored actors stole only basic information but now they are building long-term espionage campaigns and installing and using sensors in secure networks whenever possible.

Government and defense sectors in the United Arab Emirates and Saudi Arabia – the two largest economies in the Arabian Gulf – will likely be high-value targets as Iran seeks geopolitical prominence.

In a report published in March, Microsoft linked Iran hackers to cyberattacks that targeted thousands of people in more than 200 companies, including some in Saudi Arabia.

Over that six-month period, 26,800 malicious RDP behaviors were detected by the Cognito platform. Throughout the rest of this report, detection counts are normalized to the number of detections per 10,000 workloads or devices to enable comparisons between organizations of different industries and sizes.

Overall, manufacturing and finance organizations are the most exposed to malicious RDP behaviors. The top three industries together account for half (50%) of all RDP behavior detections.

For further insight, RDP behaviors were broken down by two Cognito detection types: RDP Recon and Suspicious Remote Desktop. Manufacturing organizations experienced the highest frequency of both RDP behaviors.

The three most at-risk industries for RDP Recon are manufacturing, government, and education, while the industries with the top three rates of Suspicious Remote Desktop detections are manufacturing, retail, and finance/insurance.

Industries experience variable amounts of the two RDP detections. For instance, government organizations experienced twice as many RDP Recon behaviors compared to Suspicious Remote Desktop. Retail organizations experienced the second-highest rate of Suspicious Remote Desktop detections but had the third-lowest rate of RDP Recon detections.

RDP used in real-world cyberattacks:

APT40 – State-sponsored threat actor in China

APT40 has conducted operations since 2013 in support of China's naval modernization effort.

APT40 uses compromised credentials to log-in to other connected systems and conduct reconnaissance. The group also leverages RDP, SSH, legitimate software within the victim's environment, an array of native Windows capabilities, publicly available tools, as well as custom scripts to facilitate internal reconnaissance.

APT40 uses many methods for lateral movement across an environment, including RDP. For each new system that is compromised, the group usually executes malware, performs additional reconnaissance, and steals data.

APT40 has been observed masquerading as an unmanned underwater vehicle manufacturer and has targeted universities engaged in naval research. The group has also targeted countries involved in South China Sea disputes with the Middle Kingdom, and nations China is trying to influence with its $1 trillion trade-network initiative known as *Belt and Road* across Asia, Europe and the Middle East.

This includes attacks that compromised government entities overseeing elections in Cambodia. APT40 also targeted several universities, including Pennsylvania State University and Duke University.

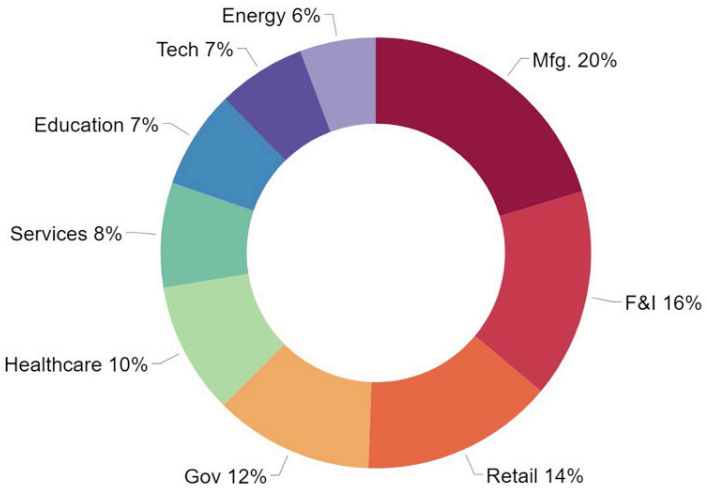

Figure 1: Distribution of all suspicious RDP behavior detections by industry

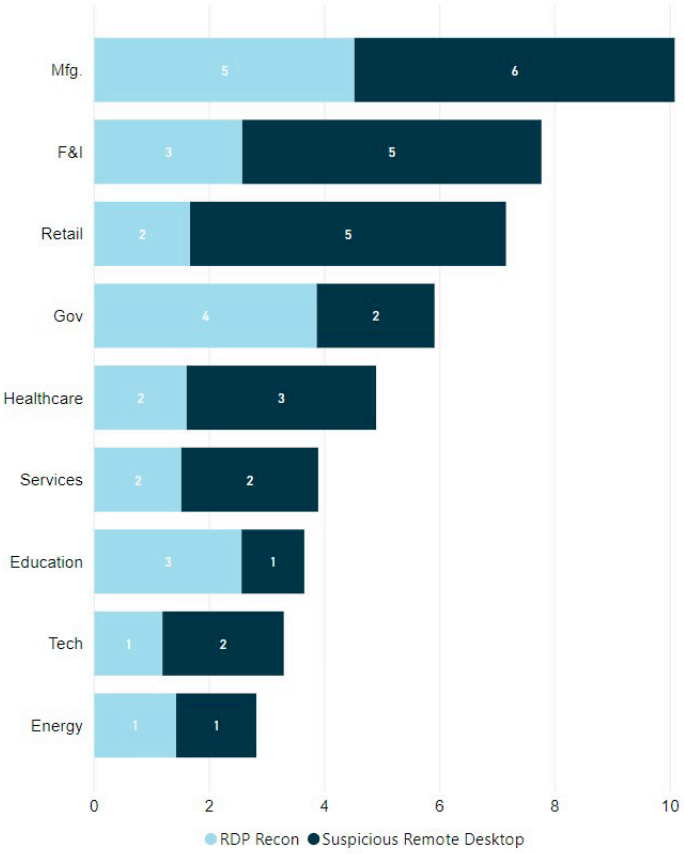

Figure 2: RDP detection type by industry per 10,000 workloads or devices

Vectra also categorized organizations by their number of employees: Small (less than 5,000 employees), medium (5,000-25,000), and large (more than 25,000). Vectra observed that across all industries, medium-sized organizations experienced the largest amount of RDP detections (7 per 10,000 workloads or devices), followed by small (6.5 per 10,000 workloads or devices) and then large organizations (4.5 per 10,000 workloads or devices).

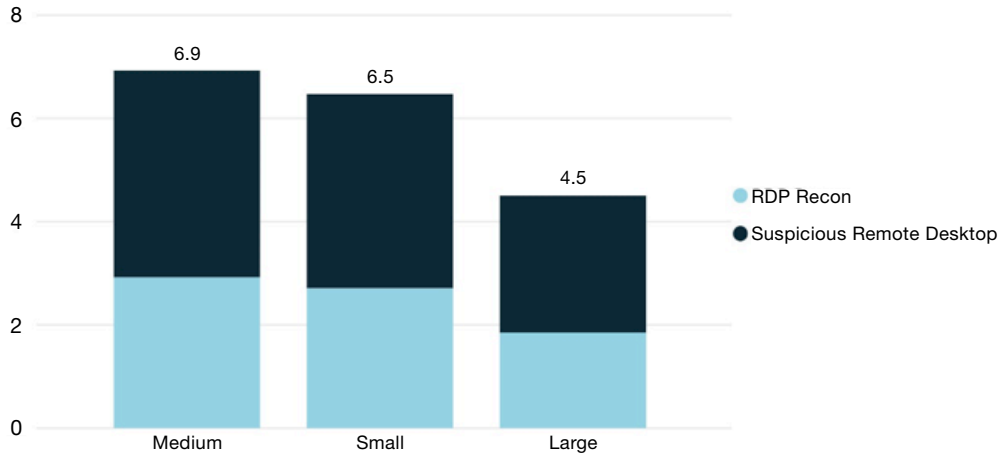

Figure 3: Rate of RDP detections per 10,000 workloads or devices by organization size

There is not a large variance of detections between medium and small organizations, but it should be noted that the largest of organizations typically have much more mature security programs with the proper staff and processes in place. This is the result of larger budgets and better access to tools and resources. We observed that the organizations with more than 25,000 employees are more likely to employ a larger staff with dedicated threat hunting, threat intelligence and incident response teams.

By combining the data on industry and company size, we start to see a more interesting picture of where RDP behaviors occur. Medium-sized manufacturing organizations, medium-sized retail organization, and small-sized finance/insurance organization exhibited the highest volume of RDP behaviors.

While the statistic does not indicate medium-sized organizations have a higher usage of RDP, it does indicate there has been more abnormal and suspicious use of RDP in those industries.

Company size is not always reflective of the number of workloads or devices. More often, industries like manufacturing have many more devices relative to the number of employees. This is a major reason why RDP is used. It enables the remote administration of physically distributed systems to achieve greater IT employee productivity. The same lean-staff approach is found in small and medium-sized retail and finance organizations.

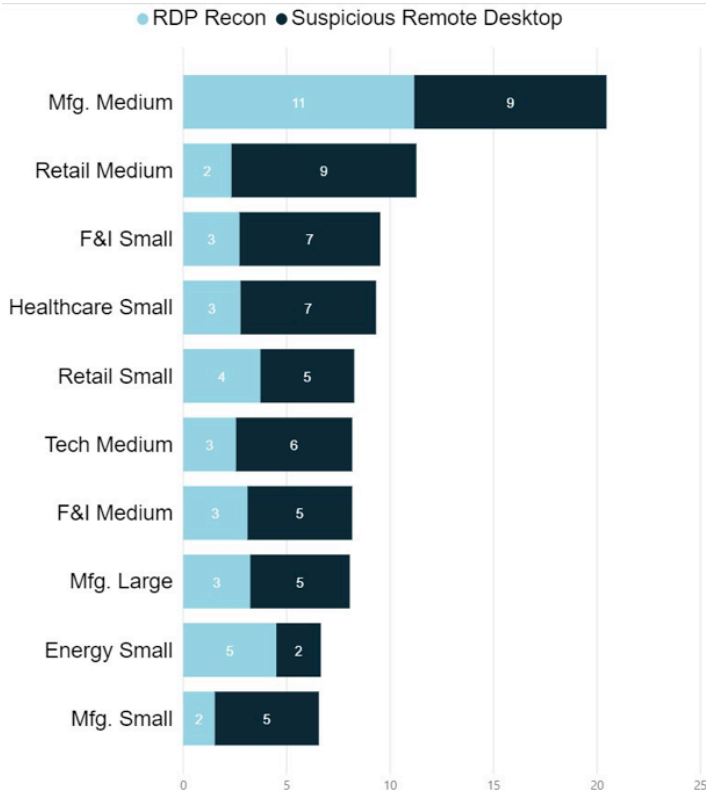

Figure 4: RDP detections per 10,000 workloads or devices by industry and organization size

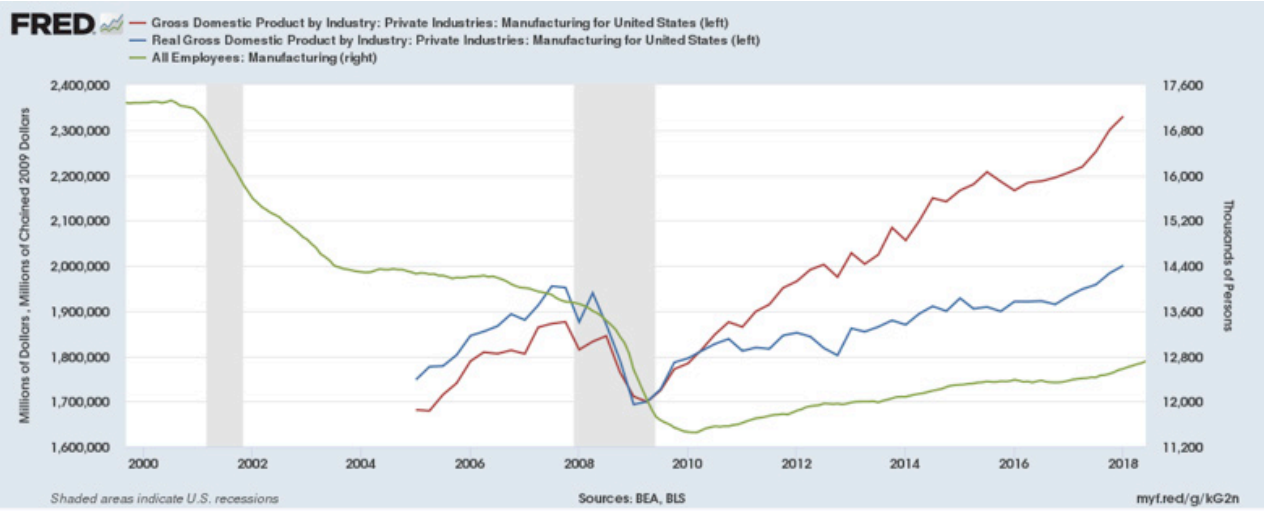

Figure 5: The increase in gross domestic product for the U.S. manufacturing industry in relation to the number of employees

Within manufacturing itself, there is a global trend for lean operations that heavily leverages technology and automation to increase output per employee. These companies usually have a small IT staff that manages a large volume of remote devices.

In companies that operate with lean staffs, it is not feasible to have personnel travel to multiple remote facilities. RDP and other remote management tools become necessary to manage many devices with a small number of IT employees. As profits for lean operations rise, companies will continue to invest in more remote management tools that increase efficiency and productivity.

Exploiting RDP in the real world

In a public service announcement, the FBI recommended "disabling RDP if it is not needed." However, it is unlikely that organizations will stop using RDP anytime soon. Many firms believe the benefits of using RDP outweigh the risks. To illustrate this point, consider the use-case of RDP in the manufacturing industry.

Manufacturers value RDP because it reduces operational costs and increases their ability to centralize data storage. Industrial manufacturing systems require close monitoring and frequent modifications. In the past, manufacturing technicians had no choice but to travel between an organization's different production plants to monitor and maintain all of them.

RDP eliminates the need for technicians to travel, saving time and money. According to Machine Design, studies show that "60% to 70% of machine problems simply require a software upgrade or changes to a few software parameters, and these can often be done remotely."

RDP used in real-world cyberattacks:
SamSam ransomware

SamSam is a computer hacking and extortion scheme that affected over 200 organizations, including critical infrastructure, hospitals and government agencies, in the United States and internationally for almost three years.

According to the U.S. Department of Justice, the cyberattackers amassed about $6 million from ransom payments, while at the same time causing over $30 million in damage as a result of the attacks.

Notable cases involved attacks on the city of Atlanta, the city of Newark, the Port of San Diego and the Kansas Heart Hospital.

The cyberattackers use RDP to gain persistent access to victims' networks. After gaining access, SamSam actors escalate privileges for administrator rights, drop malware onto the server, and run an executable file – all without victim action or authorization. RDP allowed the cyberattackers to infect victims with minimal detection.

An analysis of tools found on victims' networks indicated that the attackers purchased several stolen RDP credentials from known darknet marketplaces. An FBI analysis of the victims' access logs revealed that SamSam actors can infect a network within hours of purchasing the credentials.

While remediating infected systems, several victims found suspicious activity on their networks unrelated to SamSam. This activity is a possible indicator that the victims' credentials were stolen, sold on the darknet, and used for other illegal activity.

Technicians are now empowered to monitor systems at multiple manufacturing plants at once. The cost savings on this are substantial. HMS Networks, a supplier of industrial communication and industrial IoT solutions, estimates that each trip a technician makes onsite for a machine fix costs $2,200.

In addition to the cost savings, RDP enables data centralization. Instead of installing industrial control systems (ICS) on each employee's computer, organizations can use just one central RDP server with the ICS applications installed.

This strengthens an organization's security posture because cyberattackers who gain access to a technician's laptop still cannot access the ICS without proper RDP credentials.

Although the manufacturing industry falls victim to the highest rate of RDP exploitation, RDP also provides significant business value. IT managers in manufacturing organizations are likely to prefer the time and cost savings, as well s the productivity increase, over the abstract risk of cyberattacks.

Conclusion

The FBI's warning about the malicious use of RDP is supported by the data in this Spotlight Report.

The business value delivered by RDP will ensure its continued use and it will therefore continue to represent significant risk as an exposed attack surface.

Organizations must limit access to remote desktop management and use strong authentication. And organizations must assume compromise is possible and focus on learning the who, what, where and when of remote desktop access. This includes properly assigning user access rights and reduce instances of shared credentials so organizations can concentrate on how and when that access is used.

Monitoring remote access behaviors is essential to increase the ability to detect a cyberattacker's internal reconnaissance and lateral movement within the organization's network. Visibility into this and other attacker behaviors is dependent on the implementation of proper tools with visibility into network behaviors.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, read the 2019 Black Hat Edition of the Attacker Behavior Industry Report from Vectra.

VECTRA®
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai