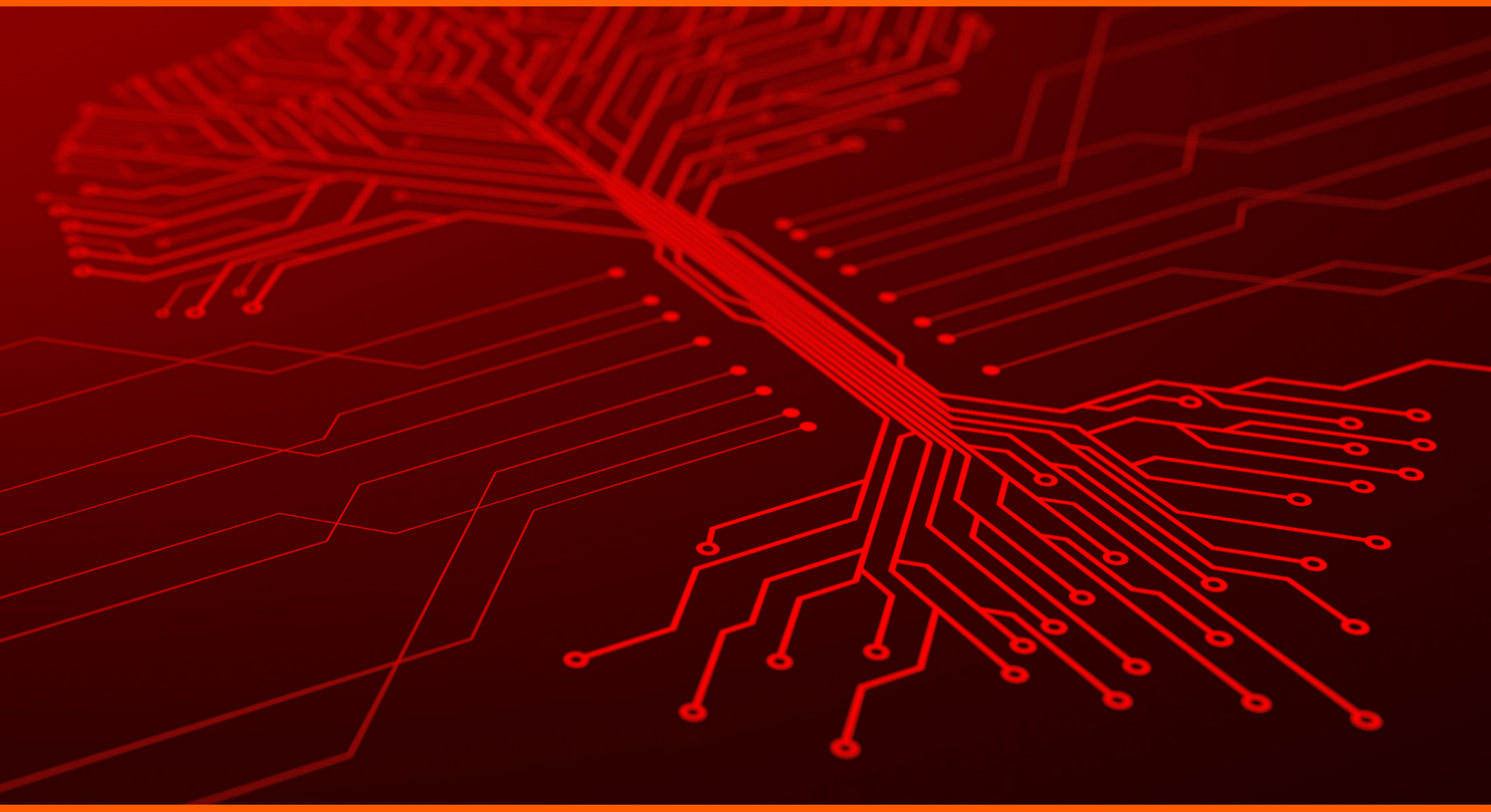
KnowBe4
Human error. Conquered.



WHITEPAPER

Root Causes of Ransomware

by Roger A. Grimes

Introduction

Ransomware is one of the biggest cybersecurity threats the world has ever faced. It is listed as THE top worry by cybersecurity professionals throughout the world, with good reason. Ransomware has attacked tens of thousands of organizations from small to very large, brought down hospitals, pipelines, food production conglomerates, police stations and even entire cities.

Emsisoft states, in 2020 alone, $18 billion was paid globally in ransom and total costs were in the hundreds of billions of dollars (https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/). Cybersecurity Ventures says ransomware will cost $20 billion in 2021 and is estimated to grow to $265 billion in damages by 2031 (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/).

The key to mitigating ransomware is to identify how it exploits devices and organizations, and then focus on decreasing the risks associated with those vulnerabilities.

The key to mitigating ransomware is understanding that ransomware is not your real problem. It is the outcome of your real problem. How ransomware gained initial access to your environment, gained privileged access and spread is the true root problem. Without the initial access, ransomware could not have successfully exploited your environment, causing operational interruption and damage.

Put another way, if you could suddenly wave a magic wand and ransomware simply went away forever, but you allowed the vulnerabilities that permit ransomware to get into your environment, you would still have a significant cybersecurity risk to your environment. Human-adversaries could still get in. Remote backdoor trojan horse programs could still get it. Keylogging trojans could still get in. Literally, the entirety of cybersecurity threats, minus one (i.e., ransomware) would still be able to take advantage of the vulnerabilities that ransomware could have used. And conversely, if you mitigate the vulnerabilities that might allow ransomware to get into your environment, you decrease the risk of not only ransomware, but every cybersecurity threat that might use the same vulnerabilities.

Fighting ransomware means identifying and mitigating how ransomware, and other malware and malicious hackers, gain the initial foothold into your environment. This paper discusses the most common root exploit methods used by ransomware to gain access into most environments.

The Root Exploit Methods Malicious Hackers and Malware Use

There are essentially nine root exploit methods that any malicious hacker or malware program can use to exploit a vulnerable device or environment. They are listed below.

- Programming Bug (patch available or not available)
- Social Engineering
- Authentication Attack
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- Third Party Reliance Issue (supply chain/vendor/partner/watering hole attack, etc.)
- Physical Attack

There is also a chance of some brand-new attack vector that is not represented here and for which no mitigations currently exist. But for now, these nine root cause methods have described the root cause exploit method used by every known malicious hacker and malware attack. In order to fight malicious hackers and malware, cybersecurity defenders need to mitigate all of these root cause exploit methods; starting by focusing on the most likely to be used root exploit methods, first and best.

The Two Most Popular Root Exploit Methods

Since the beginning of computers, just two root cause methods have accounted for the vast majority of malicious breaches to most devices and most organizations: social engineering and unpatched software. There are various other malware and hacking methods that became very popular for a few years (such as boot viruses, USB key infections, etc.), but social engineering and unpatched software have been either the number one or number two most popular exploit methods for most years over three decades.

The fact that social engineering and unpatched software are the top causes of malicious hacker and malware exploitation has been covered in hundreds of previous articles and white papers, including these examples:

- https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense
- https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
- https://blog.knowbe4.com/cyberheistnews-vol-11-14-heads-up-phishing-remains-the-most-common-form-of-attack
- https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Every organization, unless they have experience and expectations to show otherwise, could benefit by better concentrating on putting down social engineering and phishing, and better patching their environment. Doing so would best decrease the overall cybersecurity risk best and most efficiently.

What Is the Most Popular Attack Methods for Ransomware?

This paper and its related study were created to see if that fact also holds true for ransomware. Do social engineering and unpatched software stand as the primary reasons for most successful ransomware attacks, specifically, and not just more broadly for all types of malicious hackers and malware?

KnowBe4 could not survey its own customer base for the answers, because KnowBe4 customers are particularly well positioned to mitigate social engineering attacks, and that singular focus, would skew the results (i.e., our customers are compromised by social engineering less often than the general population).

Instead, to determine the most common root causes of ransomware attacks, we reviewed as many public vendor ransomware reports, news articles, and blog postings, as was possible and looked to see which detailed the exact percentages of each possible type of root cause exploit used by ransomware in a successful attack. In the research, which occurred over 3 months, we reviewed over three dozen reports, nearly a hundred news articles and dozens of blog postings.

Unfortunately, only six sources, listed below, showed exact percentages or even rankings:

- Coveware Blog Report (https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound)
- Statista (https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/)
- Forbes magazine article (https://www.forbes.com/sites/forbestechcouncil/2021/04/22/six-best-practices-for-ransomware-recovery-and-risk-mitigation/)
- Datto's Global State of the Channel Ransomware Report (https://www.datto.com/resources/dattos-2020-global-state-of-the-channel-ransomware-report)
- Hiscox Cyber Readiness Report 2021 (https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf)
- Sophos State of Ransomware 2020 Report (https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf)

Most other sources simply stated the top root causes of ransomware exploitation, but did not cover exact percentages, or did not discuss percentages at all. Almost all reports listed social engineering, unpatched software and password issues as the top causes for ransomware exploitation, but did not rank or list them against each other. Luckily, some did.

Specific Findings Summary

Here are the figures pulled from the five reports which did list ransomware root cause percentages or specific rankings:

Report Name	Social Engineering	RDP	Unpatched Software	Password Guessing	Credential Theft	Remote Server Attack	Third Party	USB	Other
Coveware Report	30%	45%	18%	-	-	-	-	-	5%
Statista	54%	20%	-	-	10%	-	-	-	-
Forbes Magazine Article	1st	3rd	2nd	-	-	-	-	-	-
Datto's Report	54%	20%	-	21%	10%	-	-	-	-
Hiscox Cyber Readiness	65%	-	28%	19%	39%	-	34%	-	-
Sophos Report	45%	9%	-	-	-	21%	9%	7%	9%
Averages	50%	24%	23%	20%	20%	21%	22%	7%	7%

Discussion

Root cause analysis is always hampered by the lack of standardization among different vendors when surveying customers or victims. Different vendors call things by different names and include different categories, which could appear in another vendor's category.

A great example of this dilemma is "RDP." RDP refers to Microsoft's Remote Desktop Protocol, which is the primary, built-in method for users and administrators to connect to a Microsoft Windows desktop. It is very common for some strains of ransomware to connect to remote login portals, such as RDP, to do password guessing. Ransomware also frequently checks for and exploits vulnerable, unpatched RDP servers and clients. One vendor could classify the latter type of RDP exploit as unpatched software and another may call it RDP. In the same vein, one vendor may call RDP password guessing, "RDP," as Coveware and Statista appear to be doing, and others may place it under "Password Guessing" only, as Hiscox is doing. And then, other vendors, such as Datto, appear to be appropriately separating them out into separate "RDP" and "Password Guessing" classifications.

Also, what does "Remote Server Attack" mean? Most of the time, that means attacking an unpatched server or some other type of exploitable vulnerability. And indeed Sophos, the vendor to report "Remote Server Attack" does not have any value in the "Unpatched Software" category. It is very likely that "Remote Server Attack" is largely attacks against unpatched software, but it could include other exploitation methods used against servers.

But the data analysis gets far messier. Most credential theft happens because of social engineering and vice-versa (https://blog.knowbe4.com/new-verizon-dbir-credentials-stolen-in-85-of-social-engineering-breaches). Three of the five reports specifically call out "Credential Theft" as a method ransomware used to compromise a victim, but it did not say how that credential theft happened. Credential theft is a possible outcome of a root cause exploit, not a root cause exploit itself. It is highly likely that credential theft, if broken down by the root cause method used to obtain the credentials was ascertained, would increase the percentages allocated to social engineering greater than the other categories.

Additionally, some vendors discussed miscellaneous root cause methods, such as USB key or simply called it "Other." One vendor reported USB key infections as possibly being involved in up to 7% of all ransomware attacks. One other vendor mentions USB key attacks as a potential method used by ransomware, but throws it under "Other," so there is no way to figure out how much is directly related to USB key attacks only.

Another vendor listed insider threats as another cause for ransomware, where either a trusted insider was bribed to install ransomware or was a direct member of a ransomware gang who planted the ransomware program. This category could be related to the USB key root causes mentioned above by one of the vendors. There have been court confirmed reports of trusted insiders being bribed, oftentimes up to $1 million, to install ransomware. Here is one example story involving Tesla, Inc.: https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/

Exploit Vector by Victim Size?

The Coveware report (https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound) has an interesting breakdown. Coveware's data show that smaller organizations are far more likely to be exploited because of software vulnerabilities and social engineering (number one and number two in order) as the chances of RDP being involved increases as the organization's size increases. For the largest organizations, social engineering goes away (it is not reported at all), and RDP is involved in over 65% of attacks and software vulnerabilities are involved in about 30% of attacks.

This is very interesting data and not something that was found in any other report. Other reports broke out various ransomware statistics and figures over different size organizations, but only Coveware did this for root causes.

Coveware's report is also the only report to consistently show RDP as the top root cause, although social engineering is sometimes number one (or number two). No other report shows RDP as the top cause in any report. This can be a direct statistic of Coveware's customer base and how it is compromised by ransomware or could reflect how other reports may categorize password guessing using RDP as "Password Guessing" and not as "RDP." Either way, Coveware has some of the most interesting and detailed data on ransomware of all vendors, even if some of it appears as an outlier.

Conclusion

Looking at all reports, whether they reported specific percentages or not, it is safe to say that social engineering is the most consistent number one root cause. Social engineering was picked as the number one reason for successful exploitation by ransomware by every report studied, except for one, the Coveware report. But even that report shows social engineering often being the top cause during some time periods. Due to the way that outcomes and root causes are commingled by most reports, it is likely that the percentages of social engineering are even higher than directly reported. This would be consistent with all malicious hackers and malware attacks, more broadly.

However, unpatched software, which is the number two most common root cause exploit for all malicious hackers and malware, drops to a distant number three (or even lower) reported ransomware root cause. This is likely due to the higher than normal involvement by several ransomware families of Microsoft's RDP.

Clearly, all organizations wishing to best reduce cybersecurity risk should mitigate social engineering and unpatched software. Organizations wishing to specifically mitigate ransomware should concentrate on those two mitigations and add mitigations against RDP and password guessing attacks.

Resources

You can best prevent social engineering and phishing attacks by using KnowBe4's products and services as part of your top mitigation tactics. For free resources on these topics, visit:

https://www.knowbe4.com/resources

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01WPSB30R01