Threat Spotlight: The untold stories of ransomware

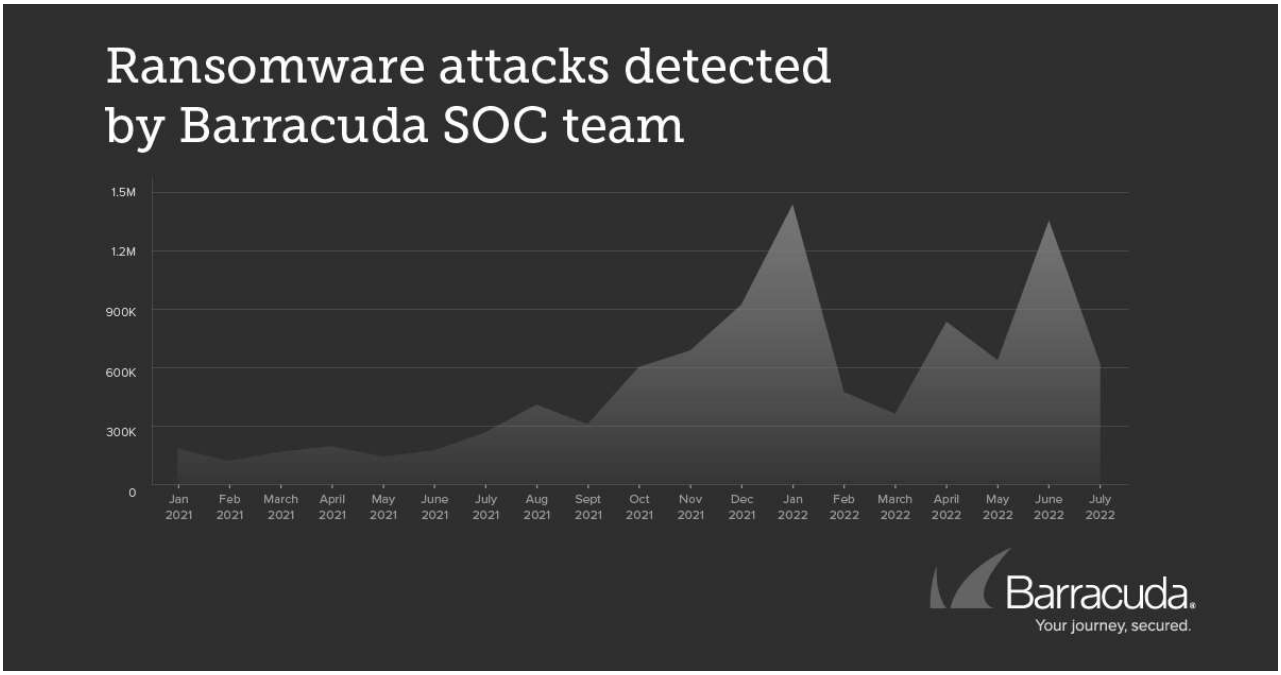
blog.barracuda.com/2022/08/24/threat-spotlight-the-untold-stories-of-ransomware

24 augustus 2022

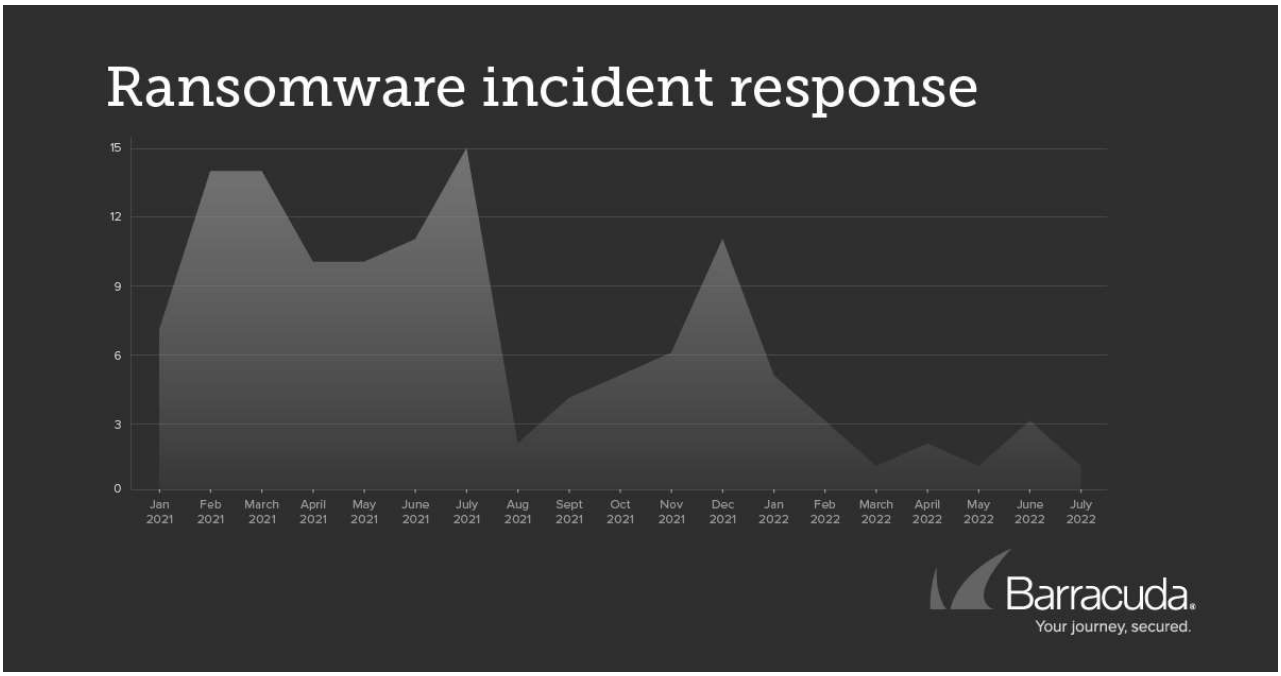
Ransomware continues to be a threat to businesses of all sizes in a year dominated by geo-political uncertainty and chaos. 2022 started with war in Ukraine, and since then the goal of many high-profile cyberattacks has turned from pure financial gain for the attackers to a desire to cause as much disruption and damage as possible.

Ransomware attacks continue to be rampant. Sometimes they turn out to be waves of wiperware. Our researchers analyzed 106 highly publicized ransomware attacks between August 2021 and July 2022 and found an increase in attacks across all of the most targeted industries, with attacks on critical infrastructure in particular quadrupling.

Beyond these large attacks that make headlines, though, there are many more small businesses quietly struggling with ransomware and trying to recover after successful attacks. To shed light onto these untold stories of ransomware, this year we also gathered data and examples from our SOC-as-a-Service team, looking at the volume of attacks the SOC has detected and the number of ransomware incidents they helped businesses address.



The volume of ransomware threats the SOC detected spiked between January and June of this year to more than 1.2 million per month. In comparison, the number of actual ransomware incidents spiked in January and then started to slow down in May.



In this Threat Spotlight, we will examine the ransomware attack patterns we identified in our analysis of attacks over this 12 month period and share our insights on prevention and recovery.

Highlighted threat

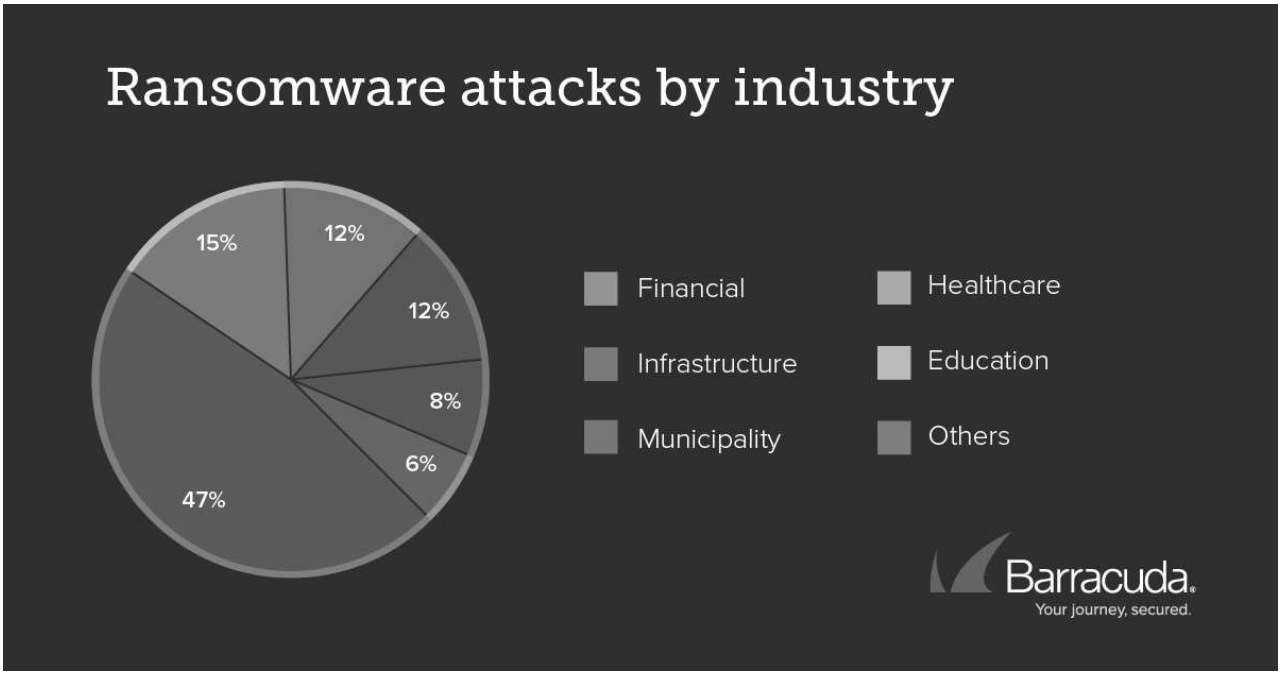
Ransomware — Cybercriminals use malicious software, often delivered as an email attachment or link, to infect the network and lock email, data, and other critical files until a ransom is paid. These evolving and sophisticated attacks are damaging and costly. They

can cripple day-to-day operations, cause chaos, and result in financial losses from downtime, ransom payments, recovery costs, and other unbudgeted and unanticipated expenses.

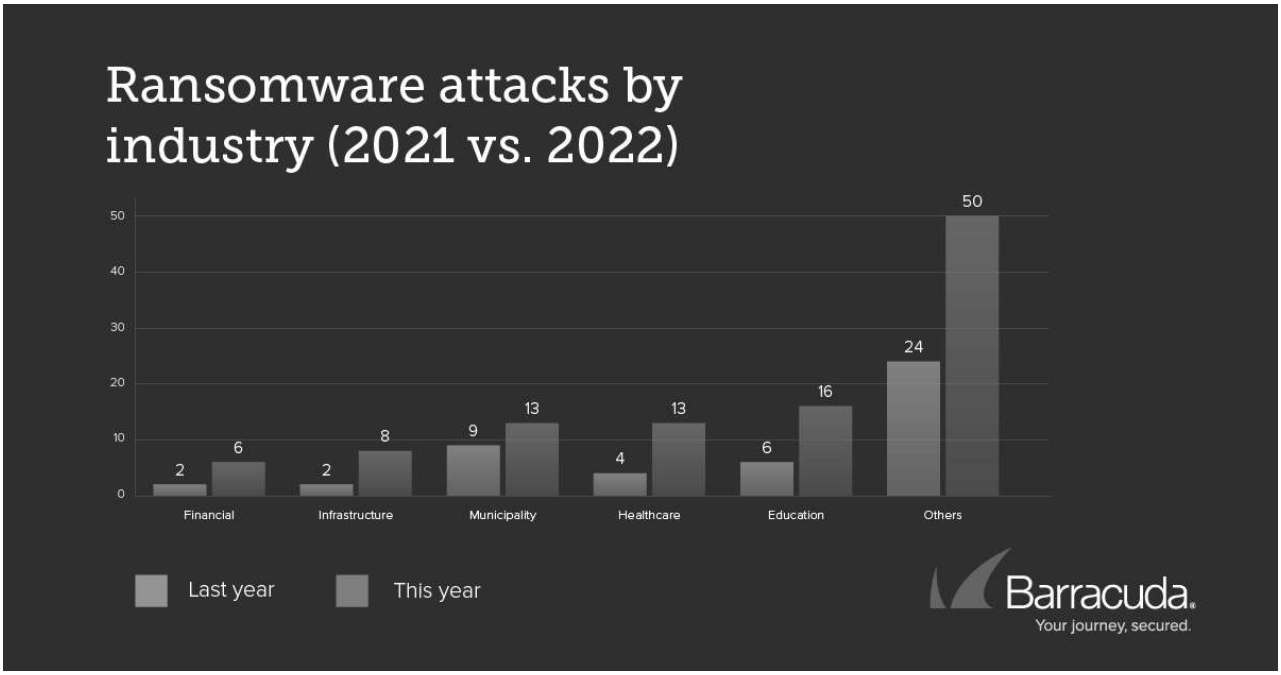
In 2021, the double extortion trend emerged, where attackers steal sensitive data from their victims and demand payment in exchange for a promise to not publish or sell the data to other criminals. In addition to that, in this year's research we found instances when attackers are now demanding a late fee or penalty if ransom payments are not made promptly.

The details

For the 106 highly publicized attacks our researchers analyzed, the dominant targets are still five key industries: education (15%), municipalities (12%), healthcare (12%), infrastructure (8%), and financial (6%).



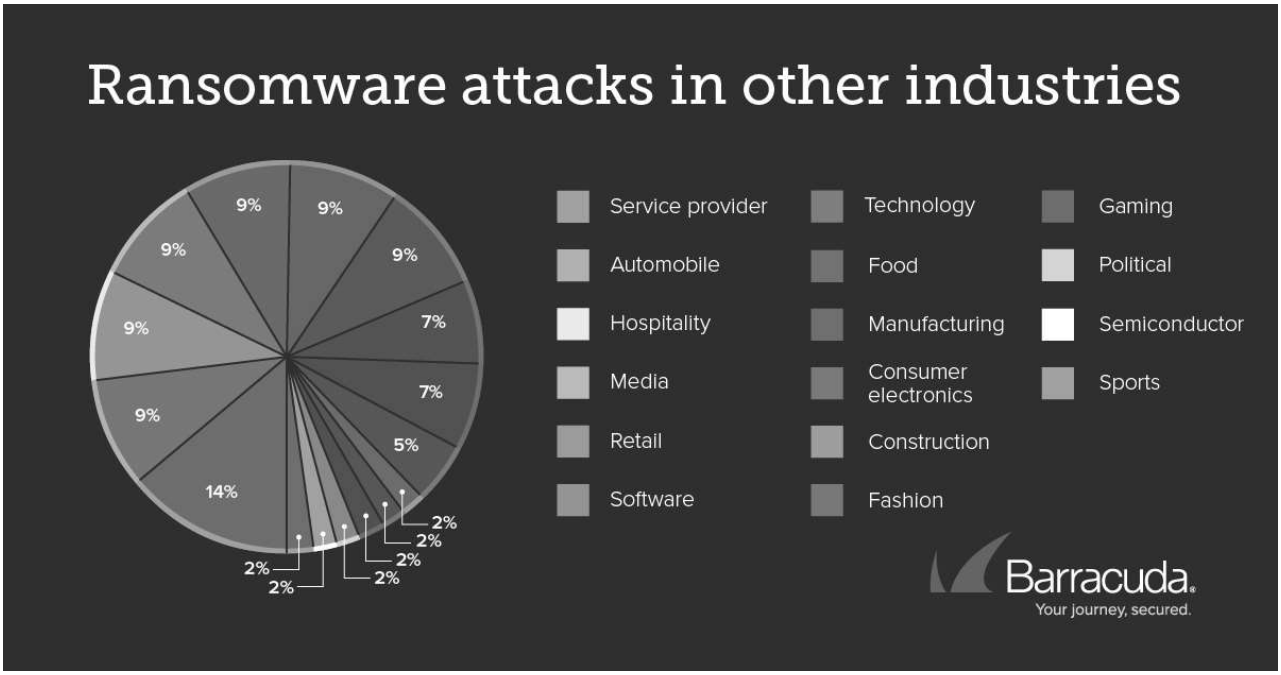
The number of ransomware attacks increased year-over-year across each of these five industry verticals, and attacks against other industries more than doubled compared to what we saw last year.



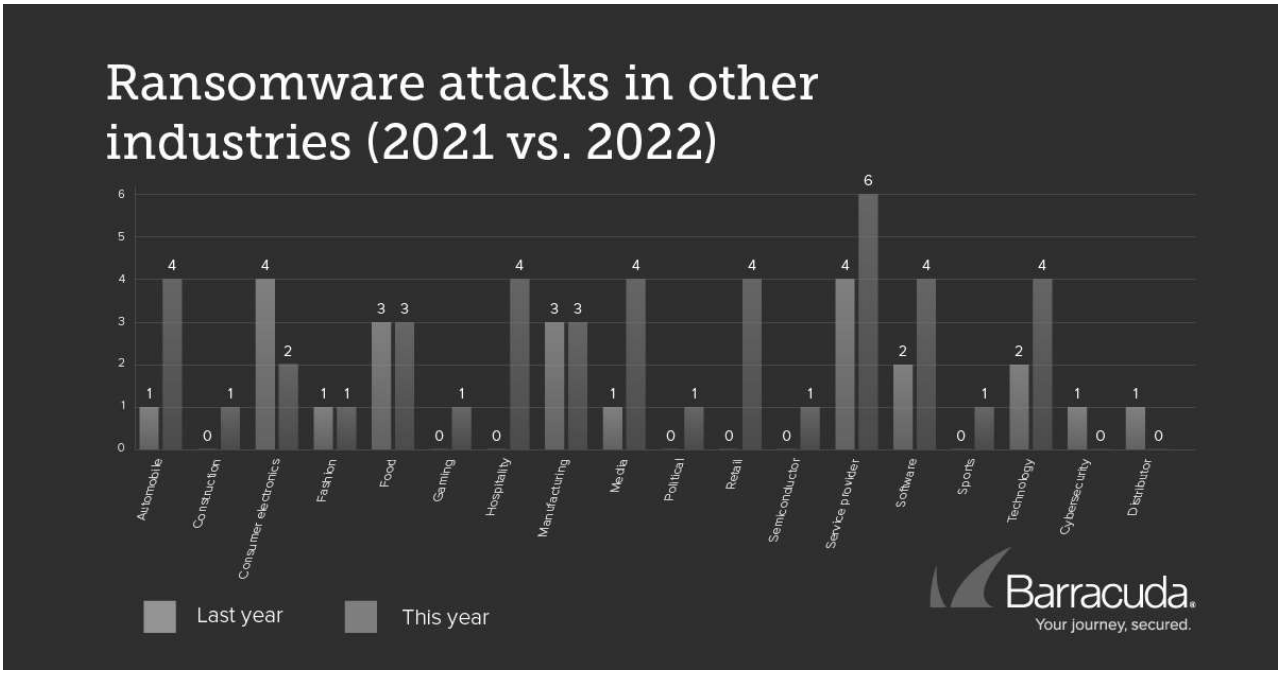
While attacks on municipalities increased only slightly, our analysis over the past 12 months showed that ransomware attacks on educational institutions more than doubled, and attacks on the healthcare and financial verticals tripled.

Infrastructure-related attacks have quadrupled, which signals cybercriminals' intent to inflict greater damage beyond the impact on the immediate victim. This leads me to realize how vulnerable we all are to potential nation-state-sponsored cyberattacks, as those are the threat actors most likely to be going after infrastructure targets.

This year, we dug in deeper on the highly publicized attacks to see which other industries are starting to be targeted. From the charts below, you can see that service providers were hit the most (14%). Whether they provide IT services or other business services, these types of organizations are attractive targets for ransomware gangs due to the nature of the access they have to their clients' systems. Access to victims multiplies if the attackers are successful in their land and expand strategy.



Ransomware attacks on automobile, hospitality, media, retail, software, and technology organizations all increased as well, and we will be monitoring them going forward.



Note, our data shows no ransomware attacks on cybersecurity companies between August 2021 and July 2022. The recently revealed attack on Cisco was not confirmed until mid-August, so it was not included in our data set.

Key takeaways

Over the past year, we've seen more ransomware payments being recovered by law enforcement agencies, as well as new levels of cooperation between the United States and the European Union to fight ransomware.

So, it surprises me to see that ransomware attackers remain defiant in the face of these government crackdowns and that they continue to operate the ransomware business with extended extortion attempts.

I'm also surprised we are still seeing a large amount of successful attacks against VPN systems without stronger authentication schemes. The rapid shift to remote work due to the COVID-19 pandemic exposed this as an area of weakness for many organizations. It makes sense that cybercriminals would continue to try to exploit these vulnerabilities, but businesses have had plenty of time to improve their authentication.

The good news is that in our analysis of highly publicized attacks, we saw fewer victims paying the ransom and more businesses standing firm thanks to better defenses, especially in attacks on critical infrastructure.

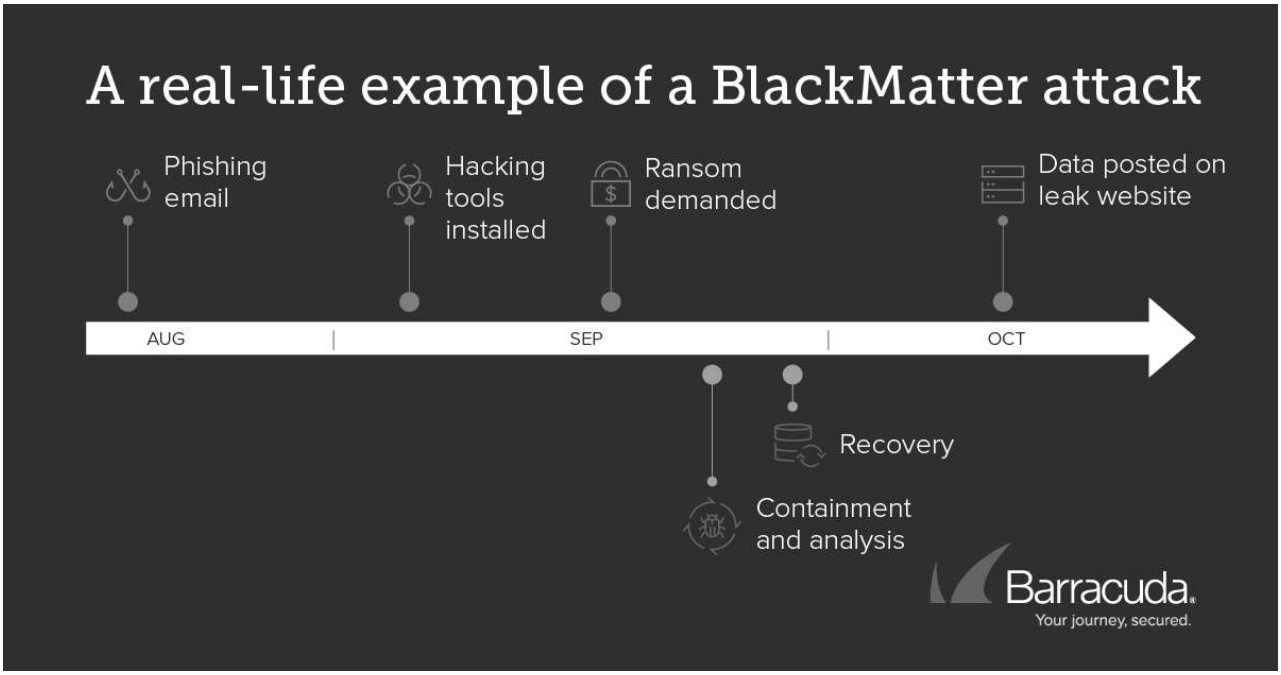
Collaboration with the FBI and other law enforcement is also making an impact. I believe the attacks on critical infrastructure were a wakeup call for authorities, pushing them to take action, and the agreements between different nation states and government leaders has created a collaborative environment for cracking down on these crimes.

3 real-life ransomware attacks

Most ransomware attacks don't make headlines, though. Many victims choose not to disclose when they get hit, and the attacks are often sophisticated and extremely hard to handle for small businesses. To get a closer look at how ransomware is affecting smaller businesses, let's walk through three examples that we've seen in our SOC-as-a-Service, go over the anatomy of each attack, and discuss solutions that could have helped stop the attacks.

Case study 1: BlackMatter

Initial threat vector: Attackers used a phishing email sent in August 2021 to compromise one of the victim's accounts. From there, they continued to expand their attack on the target by scanning and infiltrating laterally within the infrastructure, ultimately installing hacking tools and stealing data.



Ransom demand: The business received the ransom demand in September 2021 and reached out through their managed service provider for help from the SOC-as-a-Service team.

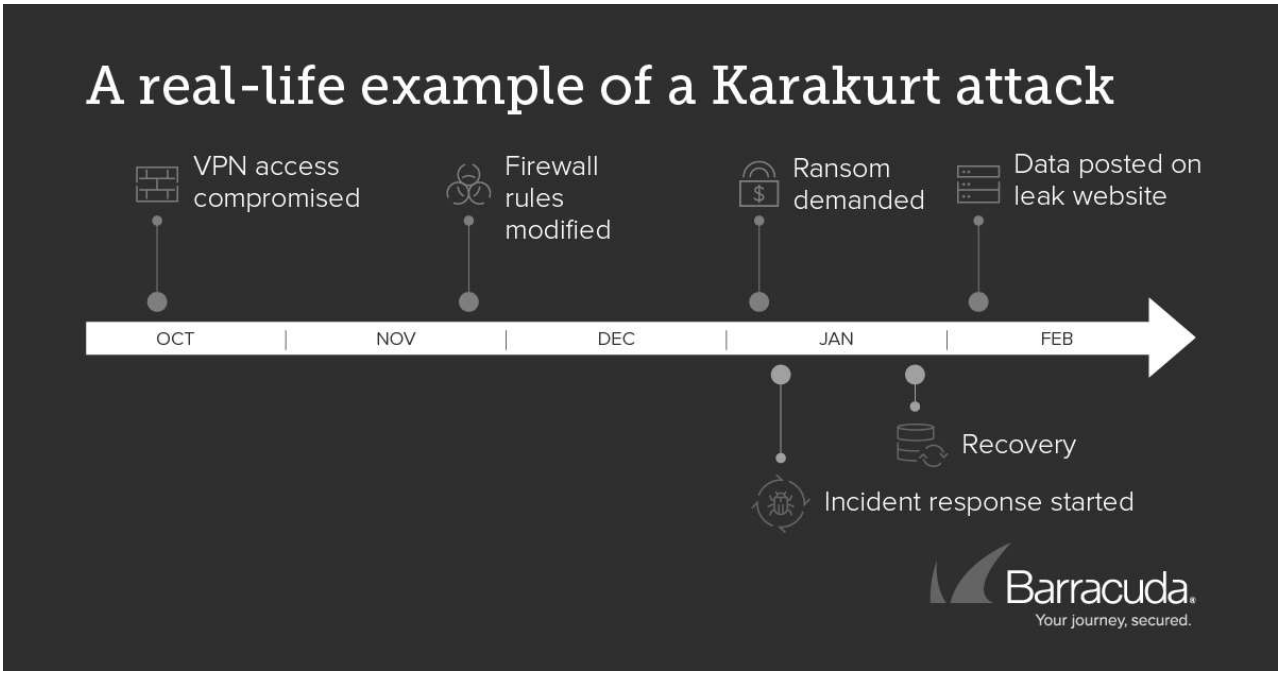
Containment & Analysis: The SOC team analyzed event logs, deployed EDR tools, isolated infected systems, and provided an FBI contact. The team also set up geo-blocking on the business' firewall, onboarded them for monitoring, and implemented a password reset.

Recovery: The encrypted machines were re-imaged from backup, and the affected machines were brought back online. A full account audit was done, and multifactor authentication was enabled.

Ransom payment: In this case the business chose to pay the ransom, negotiating down to a Bitcoin payment half of the original demand. Unfortunately, the stolen data was still leaked by the cybercriminals a few weeks later.

Case study 2: Karakurt

Initial threat vector: In October 2021 a brute force attack on a VPN login page led to the compromise of multiple domain controllers. The cybercriminals then used remote desktop protocol (RDP) to get into the compromised systems. Then in November 2021, the attackers began modifying the firewall rules.



Ransom demand: The business received the ransom demand in January 2022 and reached out through their managed service provider for help from the SOC-as-a-Service team.

Incident response: The team analyzed event logs and isolated the infected systems. Geo-blocking was set up on the firewall, and indicators of compromise (IOCs) that were found were blocked. File Storage Cloud and remote desktop apps were blocked. The customer was onboarded for monitoring, the compromised account was reset, and dedicated SIEM rules were created.

Recovery: The business worked with a third party for recovery and forensics.

Data leaked: Data stolen during the attack was leaked online in February 2022.

Case Study 3: Lockbit

Initial threat vector: The SSLVPN login page did not have multifactor authentication in place, and attackers got in with stolen credentials. The cybercriminals then used malicious PowerShell scripts and installed system-level dynamic link libraries (DLLs) to steal more credentials and harvest passwords.

In this case, multiple failures in their security posture led to more severe outcomes, including a compromised system with unsupported Windows 7, which Microsoft stopped security updates for in January 2020. A compromised administrative account led to the loss of more credentials, eventually falling to a Golden Ticket attack, which gave the attacker additional access to the domain resources while staying extremely evasive.

Ransom demand: In April 2021 the business received the ransom demand and reached out through their managed service provider for help from the SOC-as-a-Service team.

Incident response: The team analyzed event logs and public-facing servers, quarantined suspicious files, and rebuilt Active Directory.

What these attacks have in common

There are a few similarities among these attacks that it is important to recognize:

- These attacks were not single-day or single-week event. They were carried out over multiple months.
- VPN is constantly targeted. Why? Because it leads to your infrastructure and assets.
- Credentials are either stolen through phishing attacks or purchased on the dark web.
- Your email credential links with Microsoft 365 are designed for convenience, but they also mean that SSO leads to many potential routes into your infrastructure.

By overlaying the three case studies on top of the MITRE ATT&CK framework, you can see the resources and tools the attackers have. Any combination of these tools and methods could introduce challenges in defending your organization, and there are hundreds of possible combinations.

How to protect against ransomware attacks

There are five steps you can take now to protect against this type of attack:

- **Disable macros** — Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email.
- **Set up network segmentation —** Implementing robust network segmentation will help reduce the spread of ransomware if it does get into your system.
- **Remove unused or unauthorized applications** — Investigate any unauthorized software, particularly remote desktop or remote monitoring, which could be signs of compromise.
- **Enhance web application and API protection services —** Secure your web applications from malicious hackers and bad bots by enabling web application and API protection services, including distributed denial of service (DDoS) protection.
- **Reinforce access control on backups —** Backup should be offline/cloud credentials should be different than normal credentials.

Rule-based security solutions are going to be weak against these type of attacks and the ways they are evolving. As the attack surface expands, it requires artificial intelligence both to drive efficacy and to understand the behavior of these attacks.

Ransomware protection can be as easy as 1-2-3.