Ransomware Report 2022

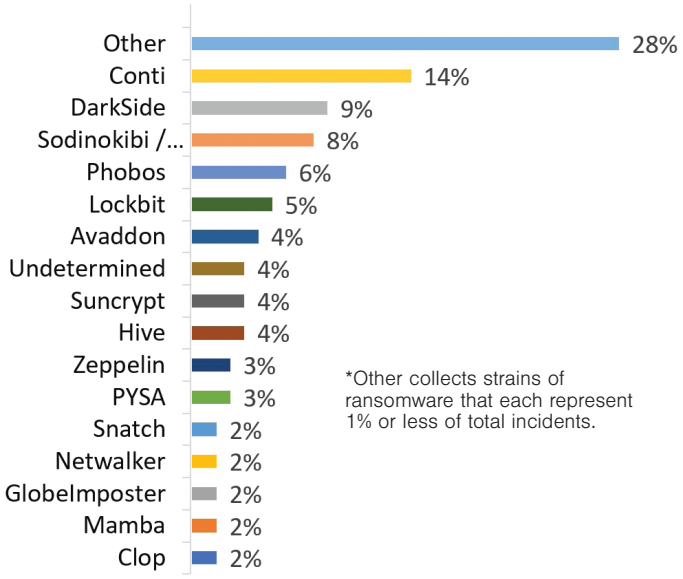
KIVU

Bracing for Chaos: What to Expect from Ransomware Next

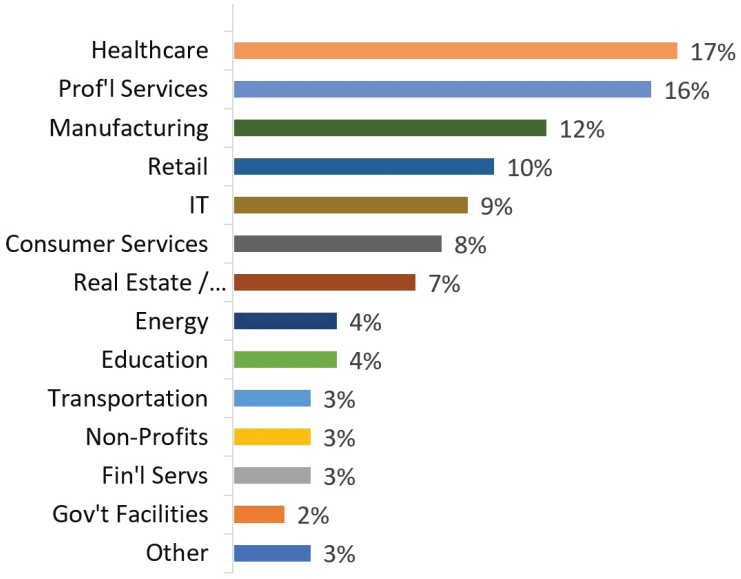
Cyber extortion is a crime of chaos. Ransomware hackers succeed when their victims are vulnerable, unprepared, and under pressure. In turn, the criminal hacker environment has grown more chaotic as well. Facing pressure from law enforcement, tightening of financial channels, and stiff competition with rival hacking groups, criminal hackers have more urgency than ever to find victims and quickly extract payments.

As we look back on another year of fervent ransomware activity, Kivu advises what these trends will mean for 2022 and sets forth how organizations can respond to manage the risk.

Kivu Ransomware Demands Paid in 2021 (% by variant)



Kivu Ransomware Demands Paid in 2021 (% by industry)



Looking Back

In 2021, Kivu observed a steady continuum of ransomware attacks that kept pace with the prior year. Kivu identified and responded to more than forty strains of ransomware. Kivu has observed that most ransomware events derive from affiliates working on behalf of their sponsors, with the opportunity for affiliates to deploy more than one strain of ransomware. Groups like Conti (19%) were significant in 2021 and continue to be active. Others announced voluntary retirements (Darkside (9%)) or were brought down by law enforcement, (Sodinokibi/Revil (7%)), and sanctions played significant roles in 2021. However, their exits provided an opportunity for new groups to emerge.

Overall, criminal ransomware groups showed a willingness to attack a broad scope of organizations, with the most significant number of victims coming from healthcare (17%), professional services (15%), and manufacturing (12%). In 2022, while Kivu expects criminal hackers to attempt discretion over their victims to stay under law enforcement's radar, most organizations remain fair game. No company should feel immune.

The Ransomware Tug-of-War

In 2021, ransomware entered at a fervent pace and only picked up steam. In addition to their steady diet of small- and mid-sized businesses, criminal hackers collected several significant paydays from large entities that brought tens of millions of dollars. Seemingly unfettered, threat actors recklessly raised the stakes. Attackers brought down critical food supply and energy companies and compromised software supply chains, leaving thousands of users vulnerable.

This escalation quickly drew a response. The White House revved up an "all-of-government" response that sanctioned ransomware groups and their financial enablers, indicted and arrested hackers, and seized their crypto assets. As law enforcement turned up the heat, threat actors scrambled to stay one step ahead. In several instances, a prominent ransomware group publicly announced its retirement, but the void from its departure was quickly filled by a highly similar group. In late 2021, Kivu observed groups like Rook and BlackCat emerge as what appeared to be such wolves disguised in the clothing of new wolves.

It has grown critical for victims to understand the nuances of these re-emerged groups. Should a victim unknowingly pay a sanctioned threat actor, that organization may still face fines and penalties. To avoid that trap, organizations must closely follow the guidance provided by the U.S. Department of the Treasury for dealing with ransomware. Due diligence should inform any payment on all available cyber threat indicators, geolocation evidence, the flow of cryptocurrency transactions, and consultation with law enforcement. These steps will provide an educated conclusion of attribution. Without sufficient due diligence, victims run the risk of deepening their problems.

Ransomware as a Service (RaaS) continues to evolve into a highly specialized and sophisticated industry. Today, ransomware developers have adopted a franchising model by outsourcing their code with little need for technical knowledge. The trend of RaaS specialization has developed to where affiliates purchase not only the code, but also the network vulnerability from a whole other source.

This specialization can create real problems for the victim. Today's threat actors require less technical expertise, and these groups often struggle to troubleshoot errors when providing their own recovery tools, downloading large quantities of data, or even protecting their own networks from cyber threats.

Moreover, as affiliates continue to splinter and represent less organized groups, those affiliates grow more independent and less predictable. Some threat actors may even go rogue from their sponsors. Unpredictable threat actors may fall through on promises, become erratic in communications, and pursue multiple extortion payments from the same victim. Kivu even observed an event with multiple threat actors sitting simultaneously in a single victim's compromised network and arguing over who was entitled to a ransom payment.

Ransomware evolved on the reputation that victims dealt with a society of "honest thieves." However, some criminal hacking groups will place less value on maintaining the benefit of the bargain. When entering ransomware negotiations, organizations need a perspective of previous events across a broad range of threat actors. By properly assessing the sophistication and reliability of the adversary, companies can develop the strategy to reach a successful outcome.

The Harassment Campaigns

Cyber extortion relies on the victim reaching a counter-intuitive concession that leaves payment as the only option. To push their victims to that point, hackers will apply pressure any way they can. Today's criminal hackers routinely subject victims to two-pronged campaigns, where systems are encrypted, and data is stolen. Even when a victim restores its network, it may still face the consequences of having sensitive data published or sold.

As the victim deliberates, threat actors will ramp up a harassment campaign. Victims, their employees, and their customers receive calls, emails, or even messages printed out by faxes and copiers that will paint a picture of chaos. In addition, communications are often released by threat actors and published online, creating a media frenzy. To overcome the pressure, victim organizations need to approach negotiations with a transactional tone and avoid further reputational damage.

More often than not, cooler heads prevail. Companies should always consider using expert negotiators like Kivu to respond to ransomware threats. By using the right expert, organizations can avoid mistakes, understand their adversary, and keep emotions in check to achieve the best result.

Looking Forward

Today, ransomware still poses an existential risk for companies to address. Despite making gains against ransomware threat actors, industry and government still have a long way to go. As more pressure is applied to hackers, Kivu expects an increase of sophisticated attacks with even greater demands.

Looking forward to 2022, companies need to build cyber resilience that accounts for evolving threats and their operations. As an essential security control, companies need to invest in endpoint detection and response (EDR), which will provide continuous monitoring of threats and update the organization on the security posture of the many laptops, mobile devices, servers, and any other internet-facing endpoint. EDR should be complemented by other vital controls like multi-factor authentication, secured and encrypted data backups, and privilege access management. Companies need to update and test their incident response plans to account for evolving ransomware tactics. By monitoring threats, testing resilience, partnering with law enforcement, and leveraging the right expertise, companies can brace for cyber incidents and be prepared for the next unknown.

Contact us to learn more at
info@kivuconsulting.com

Kivu is a leading global cybersecurity firm dedicated to offering best-in-class cybersecurity services. Since 2009, Kivu has been providing a full suite of services covering the entire incident lifecycle, specializing in the forensic response to cyberattacks and ransomware incidents.

If you are experiencing a suspected active data incident, contact us at **incidentresponse@kivuconsulting.com** or call **+1 855.548.8767.**

KIVU