TRACEPOINT

Ransomware

Where We Are and What's Next

You've heard about, read about it and if you are in the retail, manufacturing, pharma, construction or high-tech industries you have likely experienced it. Since the introduction of Maze Ransomware and their Ransomware as a Service (RaaS) model in mid-2019, the greatest virtual threat to business operations over the past two years has been ransomware. Maze blazed a path for now infamous attack groups such as REvil, Egregor, LockBit, DarkSide and many others who have exploded onto the billion-dollar scene by refining the RaaS techniques developed by their predecessor.

RaaS in short, utilizes a seemingly limitless army of individual "affiliate" attackers as virtual contractors to conduct the attack, lock down systems and steal data. The affiliate then brings the bounty back to the host group to handle the public shaming, negotiation and settlement. The affiliate then receives a portion of the crypto-currency settlement which varies by group. These groups utilize their profits to build better more sophisticated malware, employ third party services to harass the victim company and even to lease "bot-nets" to conduct Dedicated Denial of Service (DDoS) attacks against their victims. All of these tactics are employed in an effort to influence negotiations, achieve a quick settlement and recruit the best affiliate attackers to their team.

While 2020 was a banner year for ransomware, indications are that 2021 will far surpass 2020 in both the number of attacks and the illegitimate proceeds realized as a result of the attacks. Almost daily it seems, a new attack group appears which may be attributed to affiliates deciding to strike out on their own as opposed to sharing the spoils with a host group.

If you are unfamiliar with the tactics utilized by ransomware attackers you may be surprised to know that the majority of the attacks are relatively unsophisticated. The preferred attack methods of most of these criminal actors continues to be email phishing, exploiting known and unpatched vulnerabilities and credential stuffing. These attacks are aided by weak username/password configuration, lack of multi-factor authentication on both user and admin accounts, poor network configuration related to Remote Desktop Protocol (RDP) as well as Virtual Private Networks (VPNs) and inadequate protection of network data backups.

According to our research, most of the organizations who suffered an attack were not adequately prepared to respond. 75% said they were not as prepared as they had thought, with 73% stating it took too long to recover.

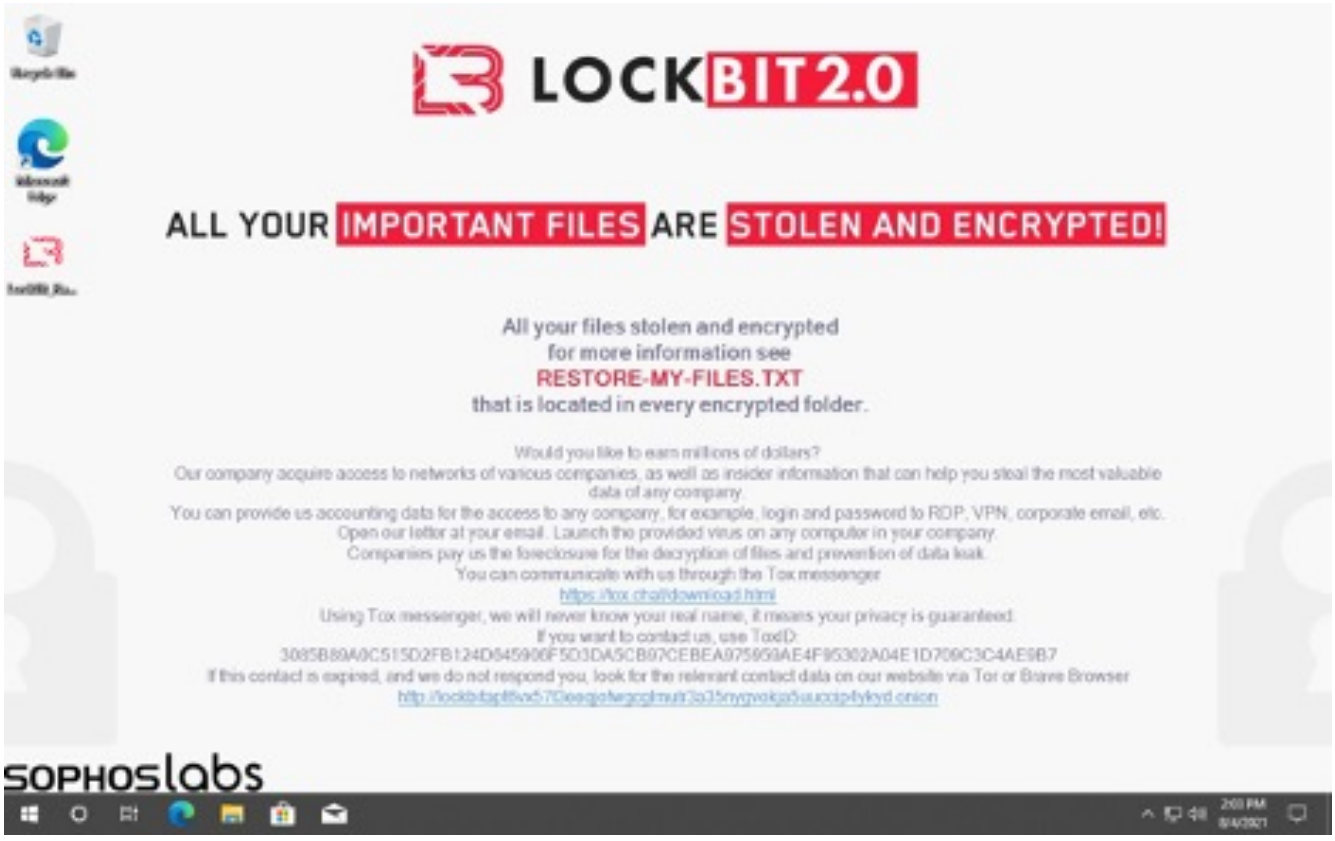
If there is a bright spot, industry executives, boards and the government are now keen on understanding the issue, the vulnerabilities and identifying solutions that provide protection against these criminal attacks. Most importantly, these entities are engaging third-party, cybersecurity firms to counsel and provide solutions in all three phases of network security (pre-breach, post-breach and network transformation/resiliency).

73% **ORGANIZATIONS SAID IT TOOK TOO LONG TO RECOVER FROM A RANSOMWARE ATTACK**

Tracepoint's proprietary research

So, what's next?

Let's assume that awareness continues to grow and true network resiliency becomes the norm, do we expect ransomware attackers to simply fade away? The answer is unfortunately no. In fact, for those who are paying close attention to the sophisticated attack groups, they have already given us a peek into their playbook for the future. Last year it was reported that the FBI had made an arrest of a foreign national who had traveled to the United States from eastern Europe to meet with an individual of a large manufacturing company. The purpose of that meeting was to offer that person a seven-figure bribe to introduce the variant locally into the company's environment. Further, the attack group LockBit 2.0 recently posted an ad that offered ordinary individuals with access to corporate environments the ability to earn "millions" of dollars to provide the same access.



Credit: https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/

70% **ORGANIZATIONS STATED IT TOOK TOO LONG TO UNCOVER THE FULL DAMAGE OF A RANSOMWARE ATTACK**

Tracepoint's proprietary research

The five pillars of protection against ransomware continue to be:

1. multi-factor authentication for all accounts,
2. segmented on-premise and off-premise backups,
3. a comprehensive patching program,
4. comprehensive email scanning/spam control protocols and
5. the deployment of an endpoint detection and monitoring solution.

However, we must embrace the reality that these attackers will employ any technique that protects their very lucrative enterprise which includes compromising a "trusted insider."

The true test of any network security program is not just the program's ability to manage known or existing threats, but rather unanticipated "over the horizon" threats. The program playbook should be routinely revisited and simulated to account for all threats. For the public or private sector entity, emerging threats are best identified through a retained relationship with a third-party provider who is actively engaged in the virtual fight and maintains vigilant visibility on these actors and their ever-changing tactics. We believe that incorporating a "trusted insider threat program" into the network security program is a critical part of protecting high value companies and government entities both now and in the future.

Unfortunately, there is no silver bullet that will stop the scourge of ransomware. Rather, the antidote resides collectively with the leadership of companies and governments to understand and embrace the issue, the vigilance of network users and defenders and with service providers to develop and provide solutions for current and emerging threats. Louis Pasteur once said "Fortune favors the prepared mind" which certainly can be argued is the sum of a capable network security program.

To learn more, contact

Bridget Q. Choi

+1 (516) 314-0269

quinn_bridget@bah.com

Nate Hall

hall_nathaniel@bah.com