What's behind the increase in ransomware attacks this year?

pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

Copy link

Andy Auld Head of Cyber Crime Intelligence, Cyber Threat Operations, PwC United Kingdom

In May, we reported a spike in cyber security incidents which had caused a significant impact on organisations already dealing with the challenges posed by the COVID-19 pandemic. Many of these incidents were the result of ransomware attacks and some of them had been accompanied by data breaches.

Since then, analysis by our Threat Intelligence team has shown that the pace and frequency of ransomware attacks have risen. In this update, we take a closer look at the trends driving the growth in these incidents.

The number of ransomware actors is increasing...

There has been a sharp increase in the number of ransomware operations this year, following a trend already established in 2019. This is likely the result of the high profile of ransomware incidents and, in cases where details of ransom payments have entered the

public domain, the perceived profitability of human-operated ransomware attacks. This is attracting new players into the market. Recent arrivals include the ransomware systems Avaddon, Darkside, Smaug and SunCrypt.

The growth in ransomware operations is not confined to new actors. Many established criminal groups have already added ransomware to their portfolios. Banking trojans such as Emotet, Dridex and TrickBot are now more commonly used as the initial delivery mechanism in highly targeted ransomware attacks. The latest threat actor to make this switch is QakBot, which since March 2020 has been used in the delivery of ProLock and DoppelPaymer ransomware.

The shift by established criminal actors towards ransomware is likely driven by opportunity costs. Successful online banking attacks rely on complex money laundering operations to receive stolen funds and transfer the proceeds to bank accounts under criminal control. The specialist criminals who provide money laundering services demand high commissions, whereas ransom payments are usually direct to cryptocurrency wallets already controlled by the attackers. As a consequence, ransomware operations are almost certainly more profitable than online banking attacks.

...because the barriers to entry are dropping

Ransomware operations can be grouped into three broad categories: private schemes, affiliate programmes and builders.

- Private schemes
- Affiliate programmes
- Ransomware-as-a-Service (RaaS)

Private schemes

We assess that several of the most significant ransomware threats, including Ryuk/Conti and WastedLocker, are run privately. They are operated by criminal enterprises whose leadership has been active for over a decade and which comprise many of the most sophisticated and experienced criminal actors we currently track.

These actors are largely secretive and do not participate in the criminal forums or marketplaces frequented by less-established actors; instead, they either have all of the resources they need in-house, or where they do need to bring in external expertise, they employ private communication channels to do so.

Affiliate programmes

Ransomware operators such as Sodinokibi, NetWalker and Nefilim are run as affiliate programmes. The threat actors are responsible for the development and management of the malware. They provide access to the ransomware to their affiliates whose role is to conduct

attacks.

The funds extorted from victims are divided between the ransomware operators and their affiliates in pre-agreed, profit-sharing arrangements. This enables actors with network intrusion and exploitation skills to acquire access to ransomware capabilities they could not easily develop themselves, reducing the barriers to entry.

Launch of the NetWalker affiliate scheme in March 2020

Ransomware-as-a-Service (RaaS)

In RaaS schemes, the developer sells access to the malware for a one-off fee. The products are usually marketed as “builders”, in that the purchaser can configure the ransomware through a graphic user interface (GUI) which then compiles the malware into a working binary. In addition to a one-off fee, some RaaS schemes offer a subscription service which provides users with “rebuilds” to reduce antivirus detections and/or updates when new features become available.

Ransomware builder on sale in criminal forums

Ransomware builder on sale in criminal forums

RaaS schemes are sold on criminal marketplaces and many are marketed as a better alternative to affiliate programmes: after the initial purchase is made, the actor keeps 100% of any revenue generated from their attacks. RaaS schemes have all but removed the entry bar to ransomware operations as all that is required to obtain a working malware package is the funds to make the purchase and access to the criminal marketplaces where they are sold.

In general, RaaS actors tend to target SMEs, whereas affiliate programmes and private ransomware operations are more likely to attack larger organisations. This is because RaaS customers often do not possess the requisite skills needed to attack and exploit large, complex networks.

Ransomware operations are scalable

The arrival of new ransomware groups, the proliferation of RaaS schemes and the fact that established criminal actors have added ransomware operations to their activities have all led to an increase in attacks. But another key factor is that many ransomware operations are inherently scalable. High-profile affiliate programmes like Sodinokibi and NetWalker have actively recruited new partners.

The income of affiliate programmes and the amount of attacks they are able to sustain are a function of the number and effectiveness of the affiliates that threat actors have recruited. This has introduced a degree of competition between rival affiliate programmes, as they try

to attract high-quality candidates to expand their operations. For example, the threat actor controlling Sodinokibi expects to retain 30-40% of the revenue generated by its affiliates, whereas a selling point of the NetWalker scheme is that successful partners can retain 80-90% of the proceeds of their attacks.

Established players are raising their game

Two of the most established and prominent ransomware threat actors have upgraded their systems in 2020. BitPaymer, a ransomware variant operated by the threat actor with the self-styled name “Evil Corp” (a.k.a. the Dridex Group), was first introduced in 2017. Although the threat actor added some incremental improvements to the code, the core system has remained largely unchanged since its introduction. In 2020, “Evil Corp” launched a new ransomware project known as WastedLocker, which was responsible for high profile attacks from the outset. Unlike BitPaymer, which was partially derived from the source code for the Dridex banking trojan, WastedLocker has been written from scratch.

Ryuk, one of the most serious ransomware threats to organisations, was first introduced in 2018. Ryuk operations were at a high tempo throughout 2019 which continued into Q1 of 2020. Since then, a new ransomware variant known as Conti has emerged. Like WastedLocker, Conti has been written from scratch, but based on coding similarities and the naming conventions used in files and commands, we assess it has been written by the threat actor in control of Ryuk.

We don't know why these high-level threat actors have introduced completely new systems, but it is likely that the rapid growth in ransomware threats has resulted in some potential targets having a better awareness of, and preparedness for, attacks. The threat actors have therefore modernised their toolsets in an attempt to retain the initiative.

Data leaks have grown exponentially

As we noted in May, the actors in control of Maze ransomware began a trend by creating a site where they posted data stolen from victims prior to the encryption of their files. The purpose of the leak site was to increase the level of coercion on new victims by making an example of those who refused to pay Maze’s ransom demands.

Since then, the number of actors with currently active leak sites has risen to 15 (or 18 if discontinued leak sites are also counted), including those in control of private ransomware systems such as DoppelPaymer, Conti and CL0P. The rate and frequency of leaks has grown rapidly, with 80% of data leaks occurring since the beginning of May.

There are risks associated with attempting to assess the level of threat posed by different ransomware actors purely on the level of activity on their leak sites:

- Leak sites normally only display data on victims who have refused to accede to the attacker's ransom demands, so it is impossible to gauge how successful individual actors are in coercing payments from victims;
- Some key ransomware actors, for example WastedLocker, do not use leak sites at all, preferring to operate beneath the radar. Others, such as ProLock are known to exfiltrate data but do not operate a leak site. However, some of these actors are likely to sell stolen information that can be used for identity theft or card fraud on specialist criminal marketplaces; and
- Attackers do not always succeed in exfiltrating data from their victims but have still encrypted their victim's files.

Nevertheless, the quantity and rate at which data is posted to leak sites may provide some insight into the scale and tempo of different ransomware operations. It is notable that Maze accounts for almost 40% of all data leaks and that they have posted data continuously since February this year. The actors in control of Conti began leaking data no earlier than the end of July, but in a little over six weeks have accounted for 13% of all leaks by ransomware actors.

Running total of data leaks since November 2019

Data leaks by ransomware operation

Conclusion

Ransomware attacks affect practically every business sector and are growing in intensity. This is fuelled by an influx of new ransomware actors, the expansion of existing affiliate schemes and the pursuit of improved revenues by established cyber crime actors. The barriers to entry into ransomware operations have been lowered by RaaS schemes which means that SMEs are as much at risk from a ransomware attack as large organisations, despite high profile incidents by "big game hunters" such as WasteLocker and DoppelPaymer grabbing the headlines.

Contact us

Contact us

Form

Hide