welivesecurity

Security news, views and insight from the ESET experts

How the threat experts see it …

BY PETER STANCIK POSTED 18 FEB 2016 - 11:49AM

The main reason for the increase in cyberattacks is that they are becoming easier, cheaper and faster to execute. Still, a cybercriminal cashes out significantly less than his or her white-hat counterpart.

These are the key findings from the **Flipping the Economics of Attacks** report, which was released this month. It is based on a survey conducted by the Ponemon Institute and commissioned by Palo Alto Networks.

The Ponemon Institute approached over 10,000 individuals with self-proclaimed hacking skills from the US, the UK and Germany who had taken part in some of the industry's events. The final sample of the survey consisted of 304 surveys, which means a 2.9 percent response rate.

The report mainly focuses on the following topics:

- the economic motivation of attackers
- why successful attacks are increasing, and
- what is the inflection point, i.e. when malicious actors quit their attack.

The economic motivation

The study shows that 69 percent[1] of attackers are motivated by money. It revealed that attackers receive on average $28,744 annually, while spending 705 hours on attacks. The authors of the paper compared this with salaries in the security industry and found out that attackers earn 29% less than the average salary for IT security practitioners in both the private and public sectors.

The data from the survey that this calculation[2] is based on is quite interesting. An attacker spends 70 hours[1] with an attack against a typical IT security infrastructure, while in the case of excellent IT security infrastructure, the number more than doubles to 147 hours[1]. The typical attacker makes 8.26[1] attacks per year with 42%[1] being successful. Of those, 59%[1] yield a non-zero return. If unsuccessful, the attack consumes 209[1] hours before ceasing. The value per successful attack is $14,711[1], while specialized hacking tools cost $1,367[1] per year.

Why successful attacks are increasing

The survey showed that attackers are benefiting from “automated hacking tools, which make it easier to execute a successful attack”. 68% of respondents strongly agreed or agreed with this statement. According to over half – 56% – of the respondents, “the time and resources incurred by hackers to execute a successful attack have decreased over time“.

As for the costs of executing cyberattacks, the extrapolated value of the decrease, as estimated by the respondents, is 25%. The main reasons are: increased number of known exploits and vulnerabilities (67% strongly agree or agree), improved hacking skills (52%), improved hacking tools (46%), improved collaboration within the hacking community (22%), as well as improved intelligence about targeted organizations (20%)[3].

When malicious actors quit their attacks

Planning and executing a cyberattack against an organization with a typical IT security infrastructure requires between one to 24 hours of time, according to 53% of the threat experts participating in the survey. The second most agreed upon timeframe to mount an attack was from 1 to 7 days (28%).

While 42% of cyberattacks are successful (this is extrapolated value; the most agreed to interval –in percentages – was from 51% to 75%, with 26% of the respondents in agreement); thus, time is the enemy of an attacker. The survey indicated that the more

time that passes before a successful attack can be executed, the more likely an organization will be able to stop it. For example, a delay of five hours in conducting a successful attack deters 13 % of attacks[1], and 20 hours deters 36% of attacks[1]. A criminal would cease an attack and move onto another target after spending less than nine days[1] on it without success.

The takeaway for the cybercriminals' targets

This survey provides unique insight into cybercriminal business tactics. However, its most crucial question – which security technologies to use to "stop or curtail attackers" – is clearly aimed at large companies (although in those cases it seems to be biased towards which solutions the study's sponsor have in their portfolio).

Seeing "threat intelligence sharing" on the pedestal of security enabling technologies, while endpoint security solutions land far behind irrelevant "hack back solutions" and obvious "honeypot solutions" is really strange.

Yes, those are all useful tools, but for larger companies, in this case, the surveyed threat experts targeted rather smaller ones. According to the report, a cyberattack – if successful – yielded only 15,000 US dollars (approximated value). This number is quite low compared to $3.8 million, which is the average total cost of a data breach as per another Ponemon Institute survey, the **2015 Cost of Data Breach Study**.

Also, small companies can make use of sharing threat intelligence, as there are advanced endpoint security solutions that contain this technology. Often referred to as Cloud Malware Protection Systems, this technology collects samples of potentially malicious applications and other possible threats for automatic sandboxing and behavioral analysis, which results in the creation of automated signatures if malicious characteristics are confirmed. All users who opt-in to use this technology thus take part in "threat intelligence sharing".

Similarly, contain other built-in technologies that are being listed as standalone technologies in Ponemon's research. With Network Attack Protection, Exploit Blocker, Advanced Memory Scanners and so on, these solutions have evolved from signature-based detection into multi-layered security solutions that cover all core needs for internet security.

Combined with effective solutions for , encryption, data backup and recovery, they make the system – while not impenetrable – secure enough to make most attacks economically unviable.

[1] this number is an "extrapolated value". Think of it as weighted average, but calculated from ranges of values instead of exact numbers.
[2] the economics of hacking calculations were based on a broad set of assumptions. For details, refer to the report.
[2] More than one response was permitted

Sign up to our newsletter

The latest security news direct to your inbox

Email...

Submit