SecureLink

SAFELY ENABLING BUSINESS

Observations from the CDC

Annual Security Report

Get the Big Picture on the real state of Cyber Security! The annual Security Report is packed full with findings from our top CDC analysts, and gives an accurate view of what happened in 2018. You get relevant information about threats, attack patterns and tendencies which build the foundation of an optimised defense for the future.

You can get the full report in all details for free on lp.securelink.net/asr!

FUNNEL:

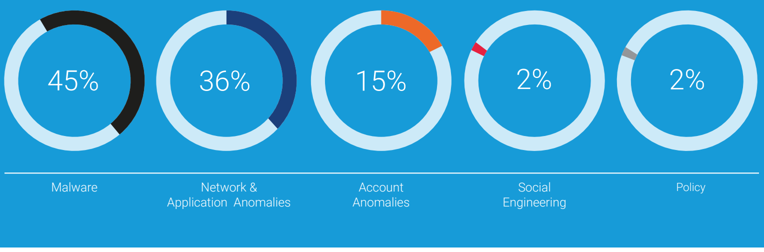
ALERT TO INCIDENT

255,701

Alerts • Use Cases • Events

21,240

Security Incidents



More than a quarter of a million incidents were tracked in our CDCs across Europe.

Over 20,000 were classified as security incidents and investigated further.

The majority of incidents were malware related, followed by network and application anomalies.

Social engineering is seemingly low, but this is likely due to the fact that social techniques prior to attacks are hard to detect. Malware or network incidents are often a consequence of successfully executed social engineering.

8% of incidents happen in small organisations with fewer than 1,000 employees, 19% happen in the mid-range (1,000 - 10,000), and the vast majority, 73%, happen in large organisations (more than 10,000).

We can see network and application anomalies dominating small and medium enterprises. But in larger organisations malware is the dominant incident type at 54%.

For companies with **under 1,000 personnel**, there's a sharp increase of incidents per head. On average, it's **five times higher** than in larger organisations.

SIZE– FACTOR

INCIDENTS PER 100 EMPLOYEES

SMALL ORGANISATIONS	MEDIUM ORGANISATIONS	LARGE ORGANISATIONS
6.8	1.5	1.3

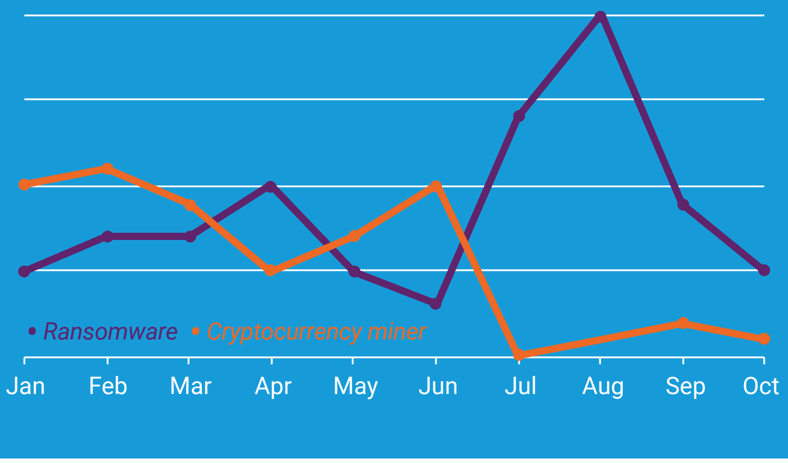
www.securelink.net
info@securelink.net

SecureLink is the market leading provider of cyber security in Europe.

SecureLink

Get the full report for free on:
lp.securelink.net/asr

RANSOMWARE
IS CRYPTOJACKING TAKING OVER?



In the last two years we have seen the rise of ransomware aimed at business: criminals hack corporate networks, destroy back-ups, and then ransom files for larger amounts.

Cryptojacking is essentially trading (stolen) computation-power into virtual currency.

It makes sense that coin mining has become popular. It's a different and far easier way to steal electronic currency than ransomware.

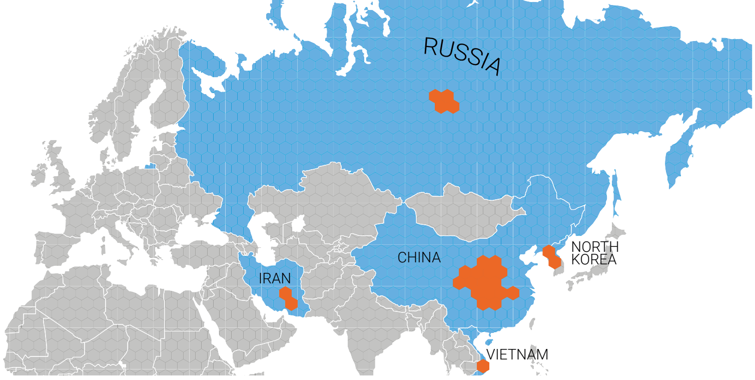
With the devaluation of electronic currency we see some criminals returning to ransomware, using more sophisticated attack schemes.

GEOPOLITICS
THE AGE OF CYBER WARFARE

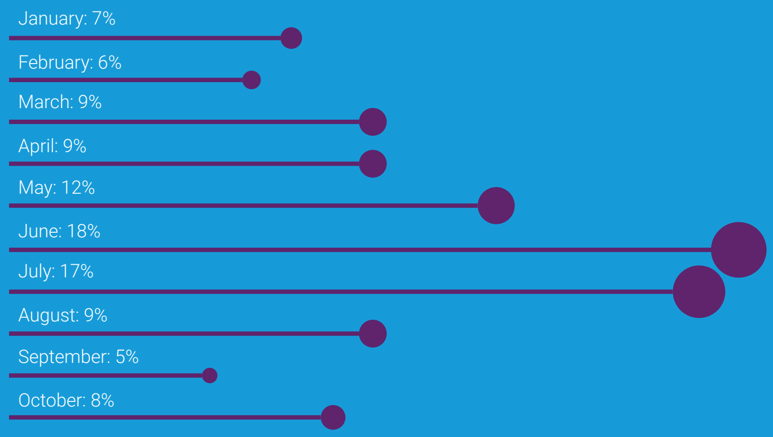
A few years ago, commoditised cybercrime was pretty much all there was.

In today's threat landscape we observe sophisticated long-term campaigns which are attributed to nation states. Aims of such campaigns vary from large scale industrial espionage to economical and even physical damage. APT groups are well funded professionals and their moves are harder to predict than those of common criminals which usually focus on financial gain exclusively.

Supply chains can amplify the damage. Though not directly targeted, corporations of any size and vertical can get caught in the crossfires, and suffer collateral damage.



SOCIAL ENGINEERING
WHY ARE WE ALWAYS FALLING FOR THIS?



Social engineering attacks distribution during 2018

From an attacker's point of view, it makes sense to focus on the behavioural patterns of humans. Technical countermeasures evolve constantly. The human, on the other hand, is much more complex, hard to predict in some situations and easy to manipulate in others.

Social engineering leverages online information to help an attacker gain intelligence about their target.

Interestingly the social engineering attempts peaked during summer. This is against the trend in general, where we see cyber criminals taking holidays along with the average population.

www.securelink.net
info@securelink.net

SecureLink is the market leading provider of cyber security in Europe.