HACKER COMBAT COMMUNITY

Hackercombat.com

Top 10 Cyber Threats Facing Businesses Today

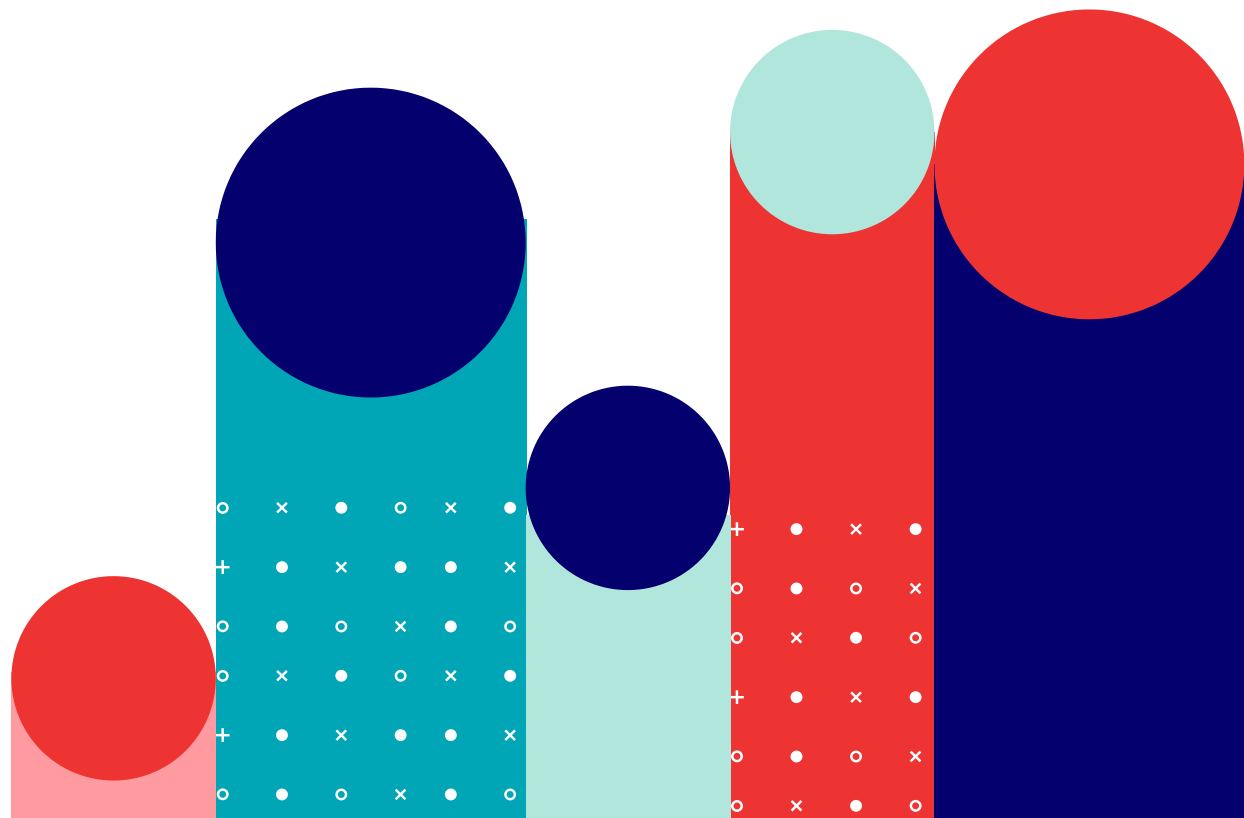
SWIPE

Ransomware

Ransomware quickly rose through the ranks of malicious applications recently as one of the more noticeable threats.

What’s alarming about this ransomware is its ability to lock down a computer and unlock it only after the owner pays a ransom. This system hi-jacking component makes ransomware very disruptive.

Attackers are spending time intelligence-gathering on their victims to ensure they can inflict maximum disruption, and ransoms are scaled up accordingly.



HACKER COMBAT COMMUNITY

2

Fileless Malware

Fileless malware gained the “fileless” moniker because it does not exist as files within the hard drive. Attackers program file-less malware to occupy the RAM. Threat analysts have a hard time finding traces of this kind of malware since it does not leave crumbs on the drive.

Fileless malware turn visible only when programmers order it to initiate the attack. Cybercriminals often deploy fileless malware against banks by inserting them into ATMs. The hackers in turn gain control of the cash machines. Another successful use hacker has for file-less malware is payload delivery. Fileless malware can unload ransomware to the system with the computer owner totally oblivious to what’s happening.

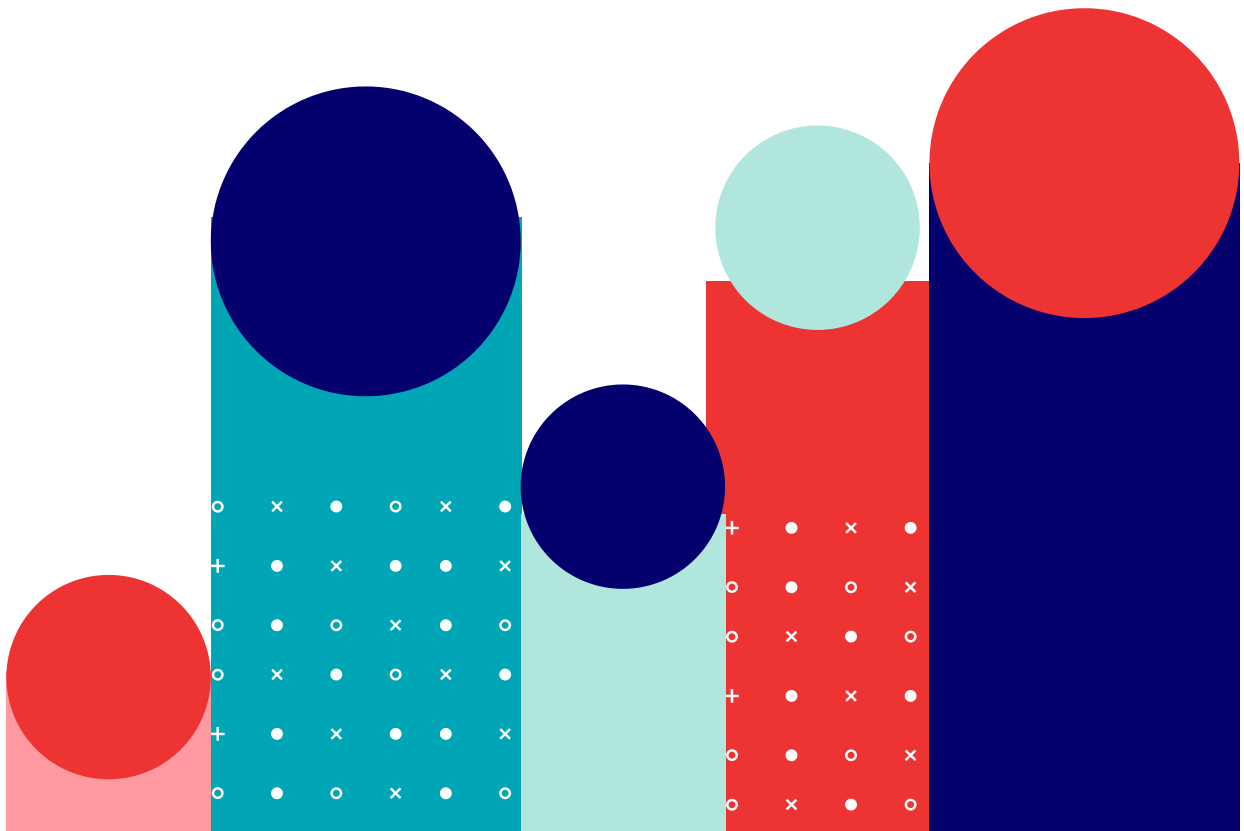
SWIPE ←

Crypto-Malware

The rise of cryptocurrencies and the explosive growth of Bitcoin in 2017 has also gained the attention of cybercriminals. Malware engineers developed malware which can actually mine cryptocurrency when the browser of an infected computer goes on the Internet.

Although not directly harmful, crypto-malware proved to be disruptive as it steals a computer's processing power to mine cryptocurrency. The infected computer bogs down and is noticeably slower in pulling up files and running programs. In time, the computer will break down because of the drain caused by the crypto-malware.

Hackercombat.com



SWIPE

4

HACKER COMBAT COMMUNITY

Zero-Day Threats

Software isn’t perfect right off the bat. Every program installs harbors security holes, called vulnerabilities, which hackers and cybercriminals can exploit. When they find a vulnerability and abuse it before the software developers can issue a fix for it, it’s considered a zero-day threat.

Once the hackers get the ball rolling and use a program’s vulnerability to deliver ransomware or inject malicious code that’s a zero-day exploit. Imagine employees opening a Word document file and then it launches ransomware onto the system.

Hackercombat.com

HACKER COMBAT COMMUNITY

Meltdown And Spectre

Meltdown and Spectre are essentially vulnerabilities inside processor chips. What merits special mention for both vulnerabilities is that because there is an inherent flaw inside processors and it exists within such a low level of the system it’s hard to defend against hackers determined to exploit it.

Hackers and malware engineers who take advantage of Meltdown and Spectre will be able to bypass current security measures without issue. They will also gain access to restricted parts of a computer’s memory and gain access to the user’s sensitive information.

SWIPE

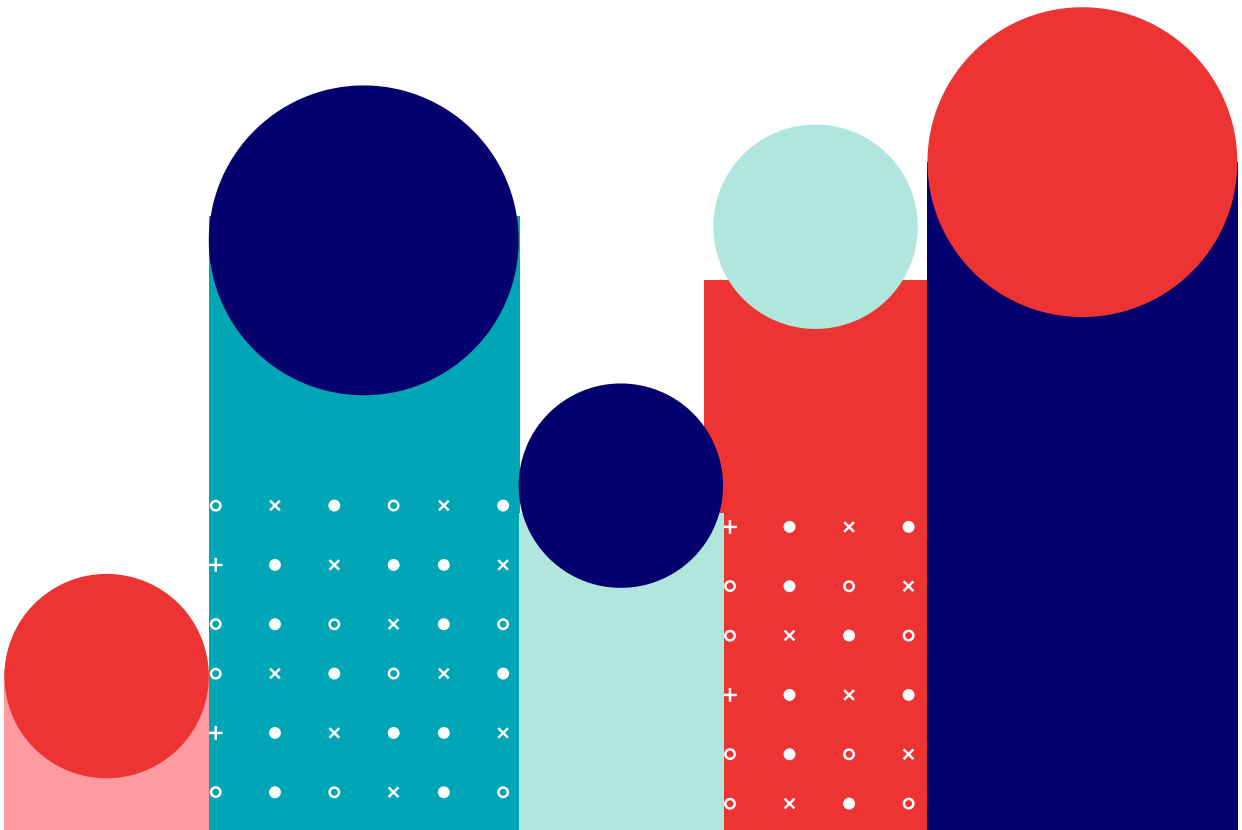
IoT Malware

HACKER COMBAT COMMUNITY

Sooner or later homes and businesses will host their own smart environments. They'll employ sensors to gain information about the temperature, use apps to control the lighting, and attach energy-efficient cameras to monitor security.

The problem is the firmware of these smart devices is also riddled with vulnerabilities. Hackers can exploit these vulnerabilities to control these smart devices. Imagine hackers switching lights off offices, halting power from flowing through smart plugs, or simply watching you from your smart surveillance system.

Hackercombat.com



SWIPE

HACKER COMBAT COMMUNITY

7

Banking Malware

Banking malware exists to steal financial information from users and deliver the information to hackers so cybercriminals can steal money from victims. Some banking malware specifically targets mobile users since smartphones now allow people to make online transactions. What's sneaky about these kinds of malware is that their authors pass them off as apps you can download for Android like battery apps or games. This type of malware will work in the background and steal your data while you're not aware.

Emotet, an incarnation of banking malware, is currently one of the more dangerous strains of malware out there. Basically, Emotet can change its form to avoid detection and then replicates itself within the system. It will move from one machine to the next by brute-forcing passwords to enter its next destination. This malware targets a user's financial information, banking details, and even their Bitcoin purses.

SWIPE ←

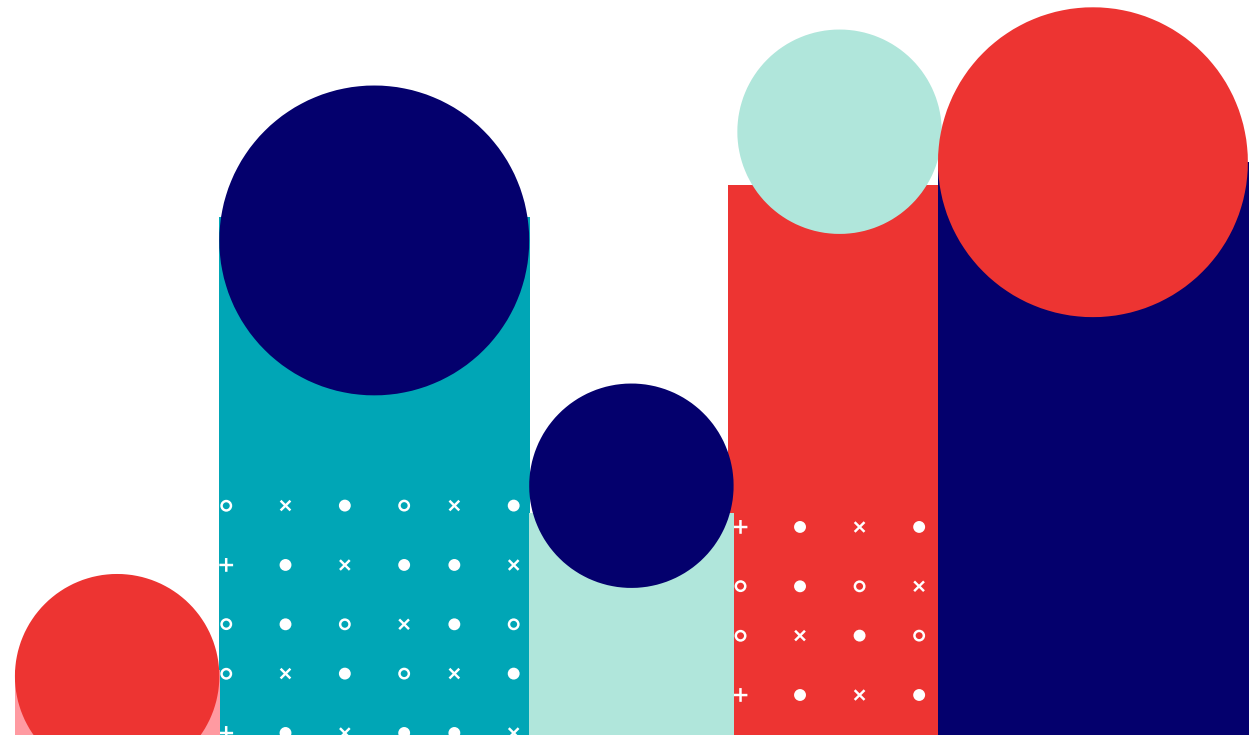
Stegware

Stegware expands malware’s attack surface. Hackers employ steganography which involves the act of hiding a malicious file inside another file, image, video, or message.

At one point only the most veteran and well-versed of cybercriminals could actually craft their own stegware. However, cybercriminals have become savvier in producing them and make stegware available through kits in the Dark Web for even the amateurs to use.

Companies will see more infections in the coming years resulting from these malicious files hiding under the cover of legitimate ones.

Hackercombat.com



SWIPE

Phishing Email

Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over $12 billion in business losses.

Some degree of data breaches happens because of human error and the form of human error which leads to a breach happens when an employee clicks on a phishing email. A phishing email often carries a payload like ransomware or a trojan horse virus which wreaks havoc on the system right after its opened.

10

HACKER COMBAT COMMUNITY

Advanced Persistent Threats

Finally, organizations should be wary of advanced persistent threats. They're what you would call a "long con" when applied to a cyber-attack.

Cybercriminals who are into APTs invest a lot of time casing their target after they've successfully infiltrated the system. Once they've gathered information, they'll start capturing and transmitting data back to their own servers.

This particular kind of attack is persistent in the sense that it can go on for years with the victim remaining unaware. Hackers who participate in APTs are dedicated professionals and often work in groups to penetrate their target organization.

Hackercombat.com

Hackercombat.com

Follow. Learn. Share

Save For Later

Follow us!

Find us Online

Like and Comment