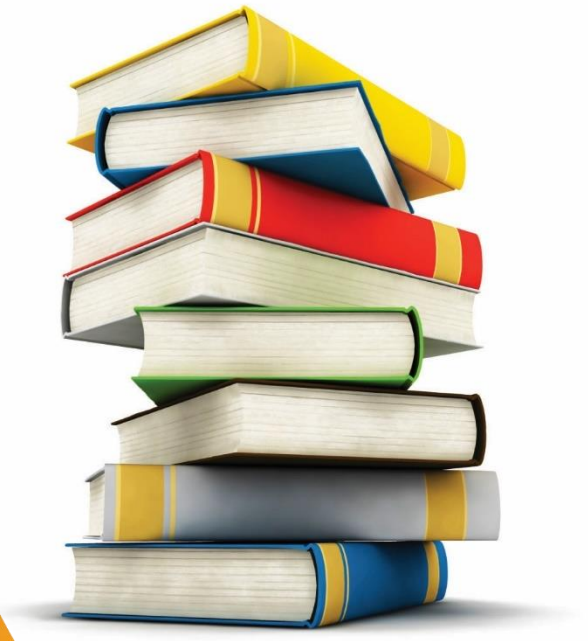
TECHNION
Israel Institute of Technology

Table of Content

Security like education is an investment, not an expense



1 | September | 2022

1. It sounds like something out of an urban legend: Some Windows XP-era laptops using 5400 RPM spinning hard drives can allegedly be forced to crash when exposed to Janet Jackson's 1989 hit "Rhythm Nation.

Microsoft Software Engineer Raymond Chen stands by the story in a blog post published earlier this week, and the vulnerability has been issued an official CVE ID by The Mitre Corporation, lending it more credibility.

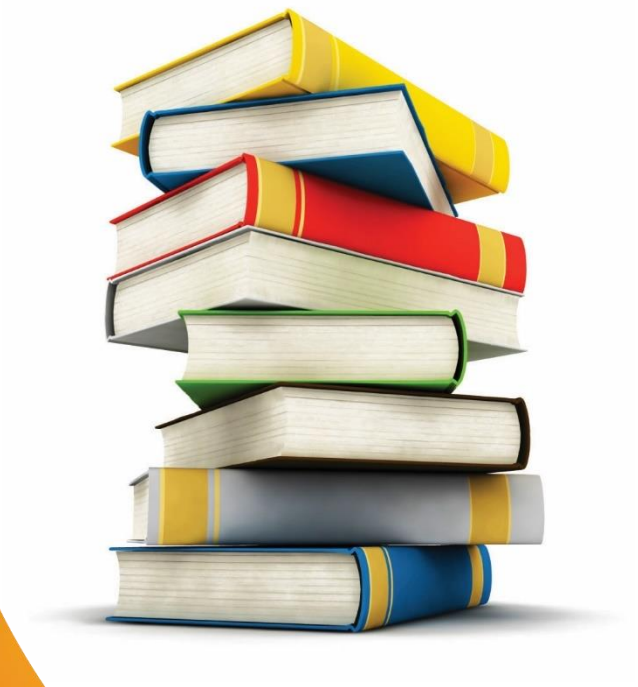
According to Chen, CVE-2022-38392 was originally discovered by "a major computer manufacturer," and it can affect not just the laptop playing the song but adjacent laptops from other PC companies as well. The specific hard drive model at issue—again from an unnamed manufacturer—would crash because "Rhythm Nation" used some of the same "natural resonant frequencies" that the drives used, interfering with their operation.
To read the complete article

What did we learn? If you still use XP-era laptop, which is not supported and not safe, here is another reason to stop using it.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

2. Counterfeit Phones with Backdoor



1 | September | 2022

Researchers Find Counterfeit Phones with Backdoor to Hack WhatsApp Accounts.

The trojans, which Doctor Web first came across in July 2022, were discovered in the system partition of at least four different smartphones: P48pro, radmi note 8, Note30u, and Mate40. Misspelling is part of the counterfeit.

These incidents are united by the fact that the attacked devices were copycats of famous brand-name models, the cybersecurity firm said in a report published today.

Moreover, instead of having one of the latest OS versions installed on them with the corresponding information displayed in the device details (for example, Android 10), they had the long outdated 4.4.2 version.
The result - they gain access to the attacked apps' files and can read chats, send spam, intercept and listen to phone calls, and execute other malicious actions, depending on the functionality of the downloaded modules.

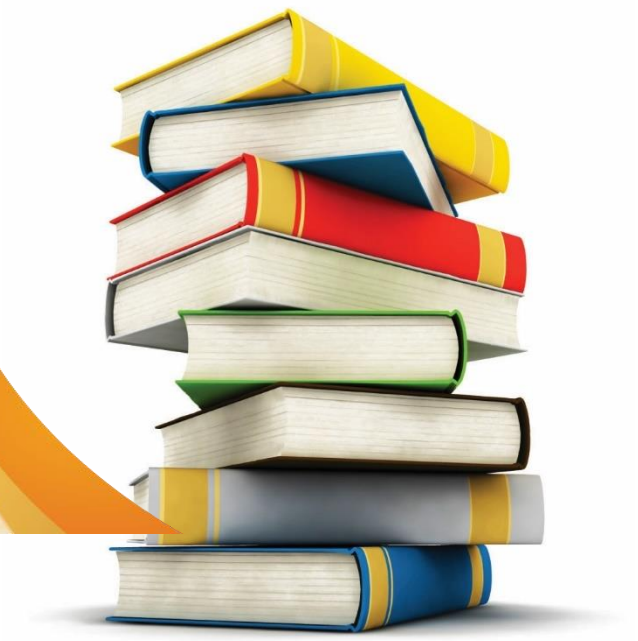
To read the complete article

What did we learn?
a. Not all smartphones are safe, some are dangerous. In security industry people with smartphones from certain manufacturers or origin are not allowed to bring them in. To avoid the risk of becoming a victim of such malware attacks, it's recommended that users purchase mobile devices only from official stores and legitimate distributors.
b. Some vendors do not provide updated software versions or security patches in time or at all. This makes the smartphone vulnerable and risky to use.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

3. Cyber war is here and now. The victims counterattack. Dostoyevsky?



LockBit gang hit by DDoS attack after threatening to leak Entrust ransomware data

1 | September | 2022

The LockBit ransomware group last week claimed responsibility for an attack on cybersecurity vendor in June. The high-profile gang is now apparently under a distributed denial-of-service (DDoS) because of it.

Azim Shukuhi, a cybersecurity researcher with Cisco's Talos threat intelligence group, wrote in a tweet over the weekend that "someone is DDoSing the Lockbit blog hard right now."

LockBitSupp, the public face of LockBit that interacts with companies and cybersecurity researchers, told Shukuhi that the group's data leak site was getting 400 requests a second from more than 1,000 servers.

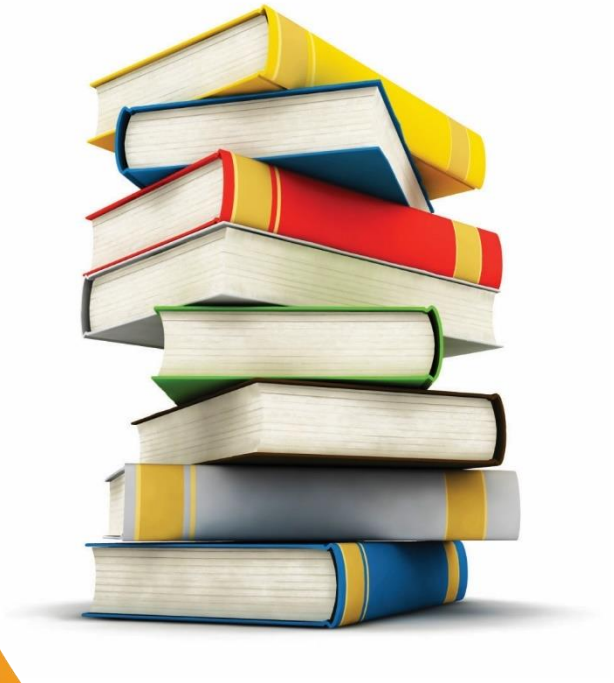
To read the complete article

What did we learn? Crime and punishment aren't just a book. Attackers should carefully choose their victims; some might hit back.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

4. The new USB Rubber Ducky is more dangerous than ever



1 | September| 2022

WHAT IS IT?

To the human eye, the USB Rubber Ducky looks like an unremarkable USB flash drive. Plug it into a computer, though, and the machine sees it as a USB keyboard — which means it accepts keystroke commands from the device just as if a person was typing them in.

Everything it types is trusted to the same degree as the user is trusted, so it takes advantage of the trust model built in, where computers have been taught to trust a human. And a computer knows that a human typically communicates with it through clicking and typing.

The new Ducky can run a test to see if it's plugged into a Windows or Mac machine and conditionally execute code appropriate to each one or disable itself if it has been connected to the wrong target.

It can steal data from the computer as well as keystrokes that include credentials.

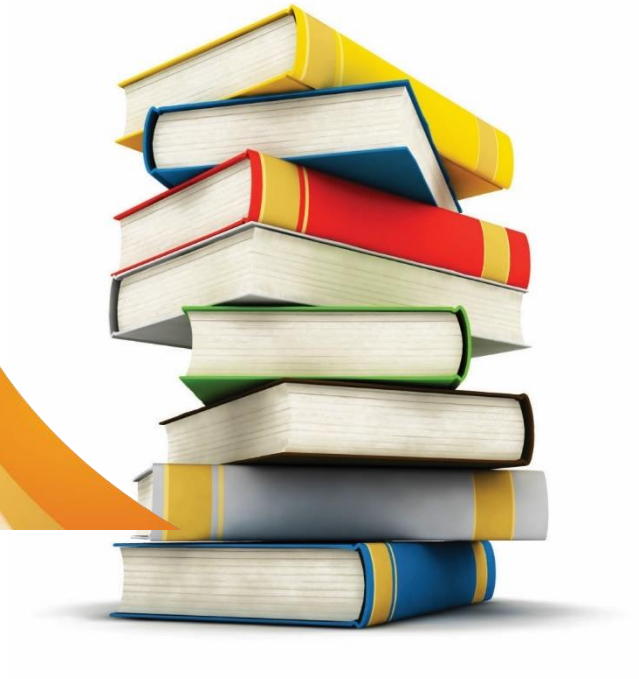
To read the complete article

What did we learn? There is no free meal. Do not plug untrusted devices into your computer.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

5. Q&A



1 | September | 2022

5. Question from the previous newsletter:

What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?
1. That the site has special high definition
2. That information entered into the site is encrypted
3. That the site is the newest version available
4. That the site is not accessible to certain computers
5. None of the above
6. Not sure

The correct answer is -2. HTTPS is more secure than HTTP

New Question

What is the best defense against ransomware?
A. Purchase comprehensive cybersecurity insurance.
B. Back up your data regularly.
C. Regularly update all your devices and software with the latest security patches.
D. Use a good Antivirus tool.

Moshe Glickstein
CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you’ve got – Don’t give it to them