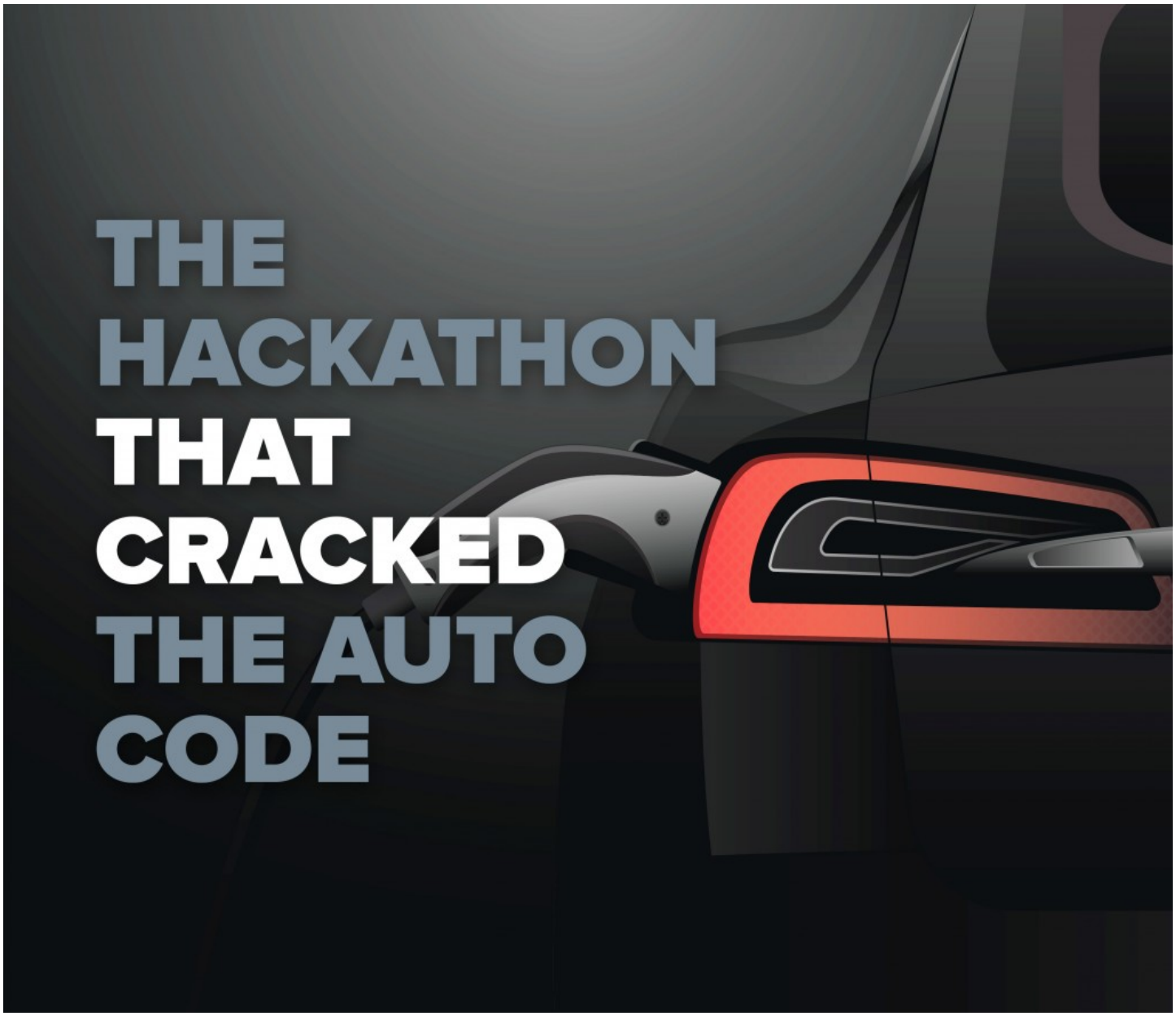
NewLinum Announces New Millennium Technology to Stop Data Breach

From automotive manufacturers to space satellites, all have experienced data breach in their computer systems to the tune of $150 Million each per year. NewLinum LLC explains new technology to make data breach a thing of history.



Austin, Texas Apr 19, 2023 (Issuewire.com**)** - Cyber tech experts have analyzed the pros and cons of a recent hacker's contest that broke into an auto maker's system. NewLinum LLC out of Austin, Texas, reviewed the contest that included the famous EV manufacturer's participation and announces its solution against malicious attacks.

SCENARIO:

On March 22nd, in Vancouver, Canada, the annual 3-day computer hacking contest 'Pwn2Own',

organized by Trend Micro's Zero Day Initiative (ZDI), revealed surprising outcomes. Cyber tech researchers and/or hackers from all over the world were invited to the event. They put their skills to the test against the highly paid cyber security executives who created the systems that protect their corporations.

According to cyber threat trend magazine DARKReading, “The participants used an isolated Tesla vehicle head unit to conduct their test. The attacks gave them deep access into subsystems controlling the vehicle's safety and other components.”

DARKReading continued, “France-based pen-testing firm Synacktiv demonstrated two separate exploits against the Tesla Model 3.”

1st Attack: “One of the exploits,” as reported in DARKReading, “involved executing what is known as a time-of-check-to-time-of-use (TOCTTOU) attack on Tesla's Gateway energy management system.”

Result: In 2 minutes, “They showed how they could then — among other things — open the front trunk or door of a Tesla Model 3 while the car was in motion.”

2nd Attack: “Synacktiv researchers exploited a heap overflow vulnerability and an out-of-bounds write error in a Bluetooth chipset to break into Tesla's infotainment system.”

Result: “Enabled them to break into Tesla's Infotainment system and gain root access to subsystems,” said DARKReading.

ANALYSIS:

According to Phil Gambell, CEO of NewLinum, “It’s only fair to say that the best cyber security experts in the world cannot identify every hole in a thought secured system. And many times, it takes a third party using unconventional means to uncover the vulnerabilities. Did the hack break Tesla’s back? Not really. As a credit to Tesla, they are wise enough to utilize contests like this, to help them improve the security of their systems. Though being hacked could be perceived as a disappointment, the last accolade goes to Tesla. They beat the hack-a-thon by using it as a benefit and came out even stronger.”

While the hackathon contest was an interesting case study, further research highlights a particular software company that can be used to protect highly sensitive data and technology.

According to Gambell, “Implementing NewLinum technology can secure an entire system. Any unforeseen flaw or weakness in a secured system, would automatically be protected and become impervious to attacks.”

Hindsight of course is easier than foresight, but there are unconventional means used to prevent attacks not only on Earth but in space as well. The NewLinum corporation recently showcased its product suite with a satellite engineering corporation to completely securitize cyber systems and prevent cyber-attacks in the space theatre.

Rico Jones, Founder and Principal Director of Space EA (Space Engineering & Acquisition Systems), operates a satellite engineering company that has over 3 decades of experience working with the DoD, NASA and recently the US Space Force. Jones will be using the NewLinum product suite to protect the most highly sensitive space technology in their planned project. Through a joint effort, Space EA and NewLinum created PAVISE.

“This solution is the only cyber security product we have found that has next generation technology. It can create a unique capability to thwart the ever-growing problem of attacks on Space Assets now and in the future”, says Jones. “And by placing secure software technology on a semiconductor chip, it can make products un-hackable, and further expand the PAVISE software solution.”

NewLinum’s technology suite has Network Access Control - a hardened network process, immune to external hacking and attacks. A methodology unique to cybersecurity, it actually changes encryptions every second, on a random basis.

“We have never seen any security technology that can deliver this type of process faster than quantum speed. This creates a hyper-secure global intranet system that provides no discernable data to any unauthorized attempt”, says Jones.

The technology has multiple proprietary protocols which enable quantum-proof secure channels of communication within the network. Since network transmissions cannot be detected, it becomes impervious to external interruptions or unwelcome intruders.

More specifically, protocols activate a random data generator, which never repeats a pattern and results in exponential algorithmic complexity and randomization. These solutions do not respond to port probes, fake IP attempts, unapproved network messages, replay, altered, or inserted messages, DDoS, and MiTM. This is part of a comprehensive solution suite that NewLinum has created to combat even a future scenario from quantum computer attacks.

“The quantum emergence threat drives a global shift to new satellite-enabled, post-quantum cybersecurity. Quantum-defying technology is the core element of secure communications infrastructures among constellations and other military assets," explains Rico Jones. "Space EA’s solution with PAVISE facilitates an intrusion-proof data exchange mechanism to overcome quantum computing threats.”

About NewLinum LLC:

NewLinum LLC is a technology development corporation in the cyber-security industry. The company's security technology suite includes post-quantum cryptography, multiple authentication systems, and dark networks – products for various applications include DEEP (Dynamically Encrypted Endpoint Protocol), Pavise, and Stealth API.

NewLinum Point of Contact: Phil Gambell, CEO - info@newlinum.com

- PWN2OWN - https://www.zerodayinitiative.com/Pwn2OwnVancouver2023Rules.html
- ZeroDayInitiative - https://www.zerodayinitiative.com/blog/2023/3/21/pwn2own-vancouver-schedule-2023
- DARKReading - https://www.darkreading.com/vulnerabilities-threats/tesla-model-3-hacked-2-minutes-pwn2own-contest

###

Media Contact

NewLinum

info@media-forest.com

512 919 6220

Source : NewLinum

See on IssueWire