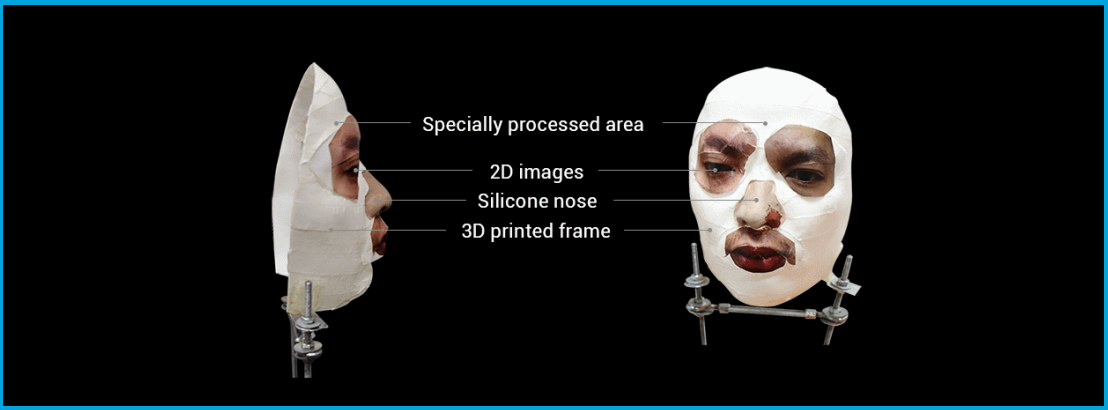
kindred

Security Newsletter

20 November 2017

Subscribe to this newsletter

Apple FaceID tricked by masks and kids



When iPhone X was launched, Apple claimed its Face ID system is unbeatable, but that turned out to be untrue when a group of hackers unlocked an iPhone X after bypassing its Face ID with a specially crafted 3D mask.

The authors of this research are experts from Vietnamese cyber-security firm Bkav, the same company that back in 2009 bypassed some of the first facial recognition systems deployed with laptops. They didn't go as far as to reconstruct accurate masks of the phone owner's face, compared to past experiments that failed. Instead, they focused on the features that needed to be valid for the actual authentication process — getting right the mask's eyes, nose, mouth, face shape, and relief. The whole process took about one week and cost researchers $150 in materials, which excludes this type of hack being used on regular users.

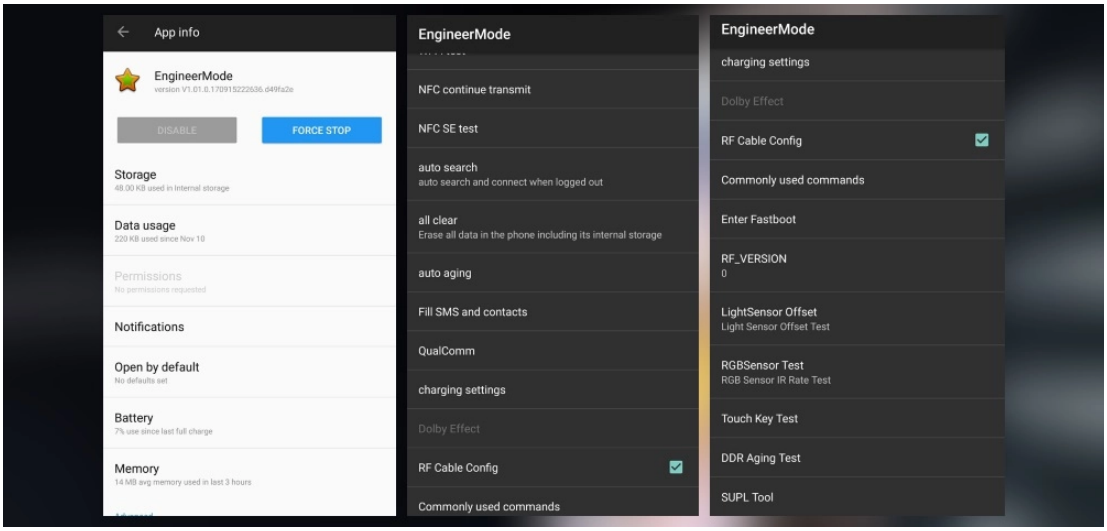
Now, a 10-year-old kid has unlocked his mother's iPhone X with his face by tricking the Face ID system proving that facial recognition is far from flawless. According to a video uploaded on YouTube, it emerged that you don't have to look alike to unlock iPhone X of your family members. Apparently, it can be done by anyone having a slight resemblance to a family member. In the video, the mom explained that she set up the Face ID with her face, but her son Ammar who naturally has a resemblance to her face was able to unlock the phone within a second.

while those discovery don't turn FaceID useless, it certainly proves the system is not as unbeatable as Apple pretended. As with any biometrics, the authentication system has a False Acceptance Rate and a False Rejection Rate, which are basically non-existent with traditional passwords. Users will have to keep this in mind while going for the convenience of those authentication systems.

FaceID tricked by a 150$ mask

10yo kid uses his face to unlock moms iPhone

OnePlus Phones Come Preinstalled With a Factory App That Can Root Devices



Some OnePlus devices, if not all, come preinstalled with an application named EngineerMode that can be used to root the device and may be converted into a fully-fledged backdoor by clever attackers. The app was discovered by a mobile security researcher who goes online by the pseudonym of Elliot Alderson — the name of the main character in the Mr. Robot TV series.

The researcher said he started investigating OnePlus devices after a story he saw online last month detailing a hidden stream of telemetry data sent by OnePlus devices to the company's servers. According to a series of tweets the researcher has published online yesterday evening, the EngineerMode app can perform a series of intrusive hardware diagnosis tests, but can also check for root status, diagnose the GPS function, and more.

The researcher says that an attacker with physical access to a phone can run the following command to root the device. Ironically, the password to root the device is Angela, name of the childhood friend of Elliot Alderson in the Mr Robot TV show.

Read More

Homeland Security Hackers Remotely Hack Boeing 757

Robert Hickey, the program manager at Department of Homeland Security's Cyber Security Division revealed that their security researchers remotely hacked a Boeing 757 parked at the airport in Atlantic City, New Jersey.

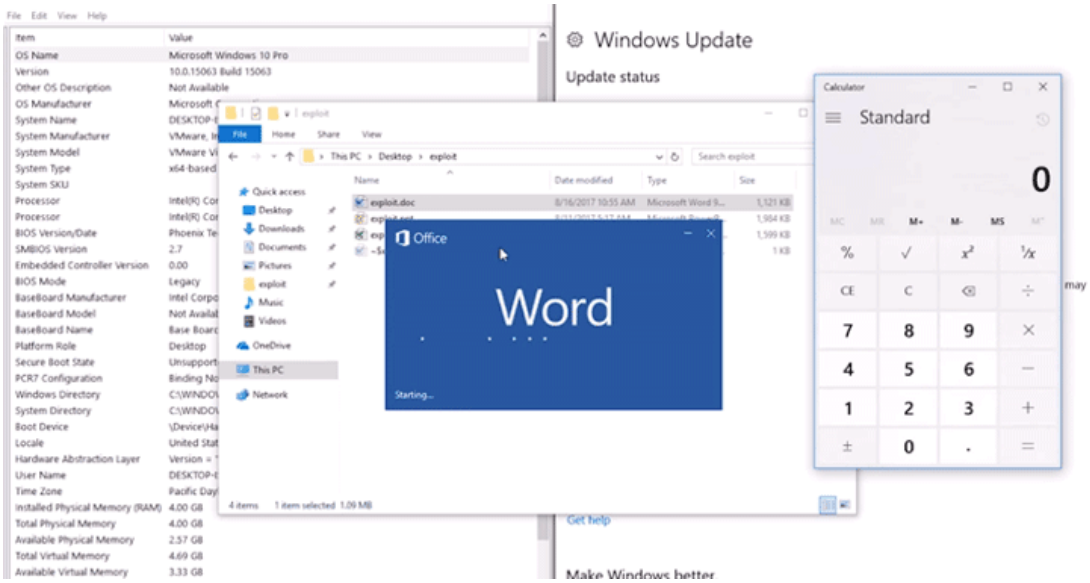
Although technical details for the hack haven't been released yet, Hickey said his team was able to breach the system's security by exploiting flaws in 757's "radio frequency communications." Although technical details for the hack haven't been released yet, Hickey said his team was able to breach the system's security by exploiting flaws in 757's "radio frequency communications." The first reaction of his team was "We've known that for years,'" and, "It's not a big deal". However, when a group of pilots from Delta and American Airlines was briefed about the vulnerabilities, they were clueless. "All seven of them broke their jaw hitting the table,

What's more shocking according to Hickey is that 90% of the commercial planes don't have protections while only new models of 737s and 787 and the Airbus Group A350 have been designed with security in mind. In a comment to CBS, Boeing said that "We firmly believe that the test did not identify any cyber vulnerabilities in the 757 or any other Boeing aircraft." Meanwhile, Hickey said research into aircraft security is ongoing. Homeland Security has yet to formulate specific advice for airplane manufacturers and airlines. Hickey also pointed out that patching avionics subsystem on every aircraft when a vulnerability is discovered is cost prohibitive

Read More

How can airlines stop hackers pwning planes over the air?

17-Year-Old MS Office Flaw Lets Hackers Install Malware Without User Interaction



Microsoft has patched today a huge security hole in Microsoft Office that could be exploited to run malicious code without user interaction on all Windows versions released in the past 17 years. Discovered by the Embedi research team, the vulnerability affects the Microsoft Equation Editor (EQNEDT32.EXE), one of the executables that is installed on users' computers with the Office suite.

This tool, as the name obviously implies, allows users to embed mathematical equations inside Office documents as dynamic OLE objects. Embedi discovered that Microsoft was still using a version of the EQNEDT32.EXE file that was compiled on November 9, 2000. the EQNEDT32.EXE component spawned its own process, outside the main Office process, that did not utilize any of the security features added to Windows 10 or the Office suite. Using Microsoft's own BinScope binary verification tool, it didn't take long for researchers to find two memory corruption (buffer overflow) vulnerabilities in the EQNEDT32.EXE file.

The exploitation chain Embedi experts devised worked on all Microsoft Office versions (including Microsoft Office 365), and with all the Microsoft Windows versions released in the past 17 years. In addition, it worked on all types of architectures (32-bit and 64-bit), did not interrupt the user's Microsoft Office workflow, and did not require any user interaction. The vulnerability — tracked as CVE-2017-11882 — was patched today in the November 2017 Patch Tuesday updates.

Last but not least, users can use two registry keys to disable registering of the legacy equation editor component in the Windows registry. The vulnerability, as described by Embedi researchers, is a gold mine for both APT groups and day-to-day malware distribution campaigns. We've certainly not heard the last of CVE-2017-11882.

Read More

Even More

Trump administration releases rules on disclosing security flaws

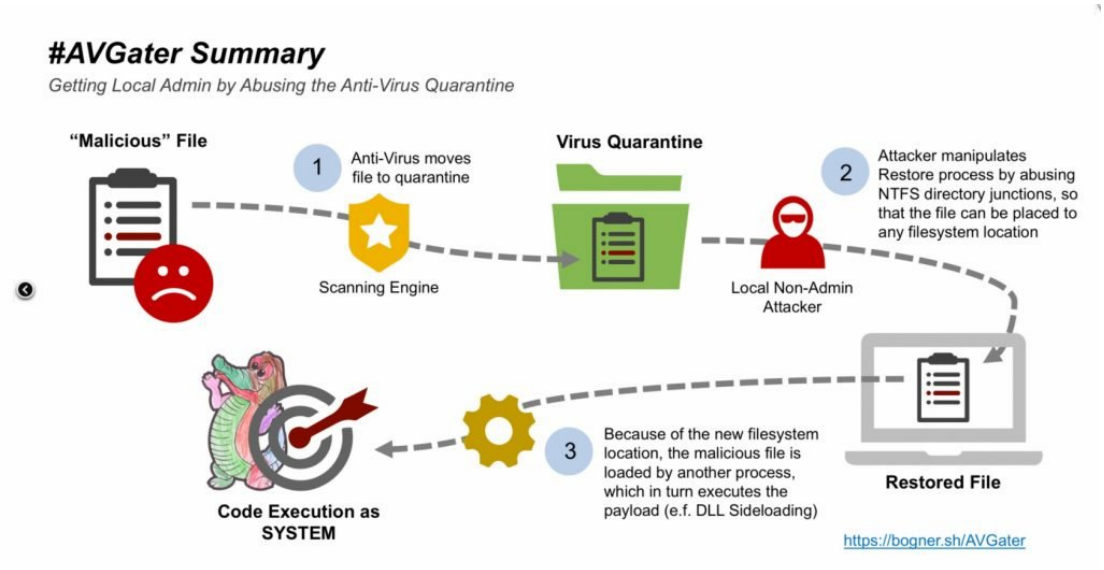
The Trump administration has released an unclassified set of rules for deciding if a security vulnerability should be shared or kept private. The White House's cybersecurity coordinator said the rules are "vital" to ensuring a balance between public disclosure and retaining flaws for intelligence operations.

Under the Obama administration, the government created the multi-agency review board to weigh if a flaw discovered by the intelligence community should be disclosed privately to tech companies, or kept a secret so that they can be used for carrying out intelligence operations, such as hacking and network exploitation.

The newly-revealed rules show that if the board decides to keep a vulnerability private, the board must reassess its decision every year. The security community, which has been calling on the government to release the details of this process for years, has long believed that the government was holding onto more exploits than it was disclosing. The unclassified report comes less than a year after a set of NSA hacking tools were stolen, and used to launch a large scale, global ransomware attack.

Read More

AVGater: New Vulnerability Exploits Antivirus Programs to Install Malware



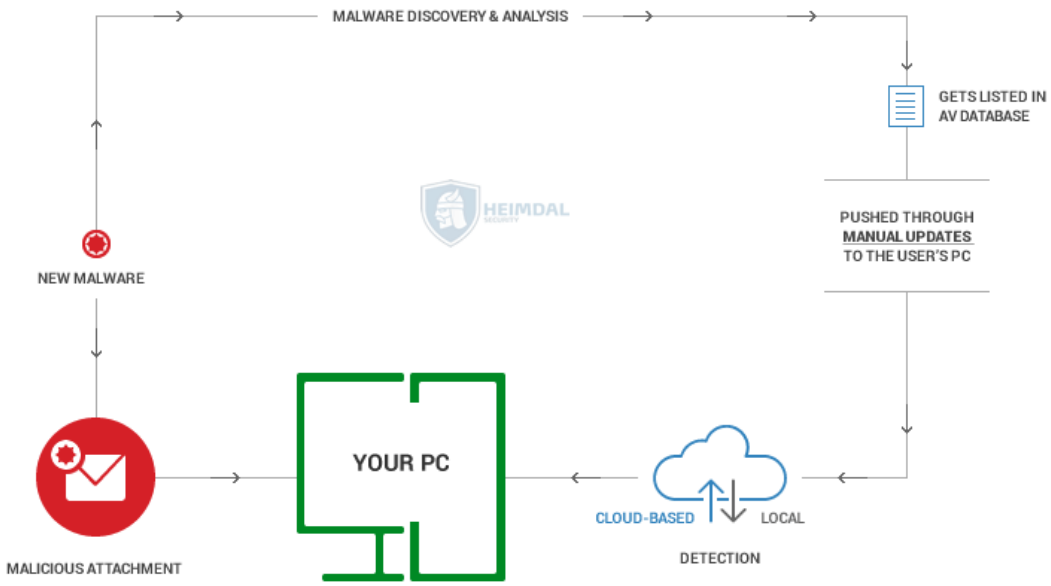
Hackers have learned to exploit the Restore from Quarantine feature, and a number of AV solutions have been affected. The flaw has been named AVGater. Once it is on a system, this vulnerability relocates malware from an AV quarantine folder and stores it to another sensitive location.

It was also possible to exploit the Dynamic Link Library search order function so that malware could obtain full privileges. A key limitation associated with AVGater is that to launch it attackers need to obtain physical access to a computer and in shared computer environments attack becomes a lot more difficult.

To prevent AVGater, users need to update the antivirus programs installed on their devices. On the contrary, enterprise computer is more at risk to this attack and therefore, Bogner suggests that enterprise users must remove the restore files from quarantine feature for good.

Read More

Why AV Detection for New Malware Remains Low



This year we saw massive spam campaigns like NonPetya or Locky fly below the radar of antivirus software and went undetected during the first hours or even days. Some of them actually went undetected even for months.

Second-generation malware usually has the ability to evade detection and bypass antivirus programs users have installed on their computers to keep their data safe. Maybe you've never asked yourself this, but do you know how long it takes for antivirus programs to detect advanced types of malware?

In this article we'll show you several examples of spam campaigns which went undetected by antivirus software and explain why this happens in the first place. We'll also provide details on how you can protect efficiently against such threats and close the various security gaps in your system.

Read More

Cutting room floor

- PCI Council Developing Software Framework
- New Vulnerability Exploits Antivirus Programs to Install Malware
- Fileless Attacks Ten Times More Likely to Succeed (Report)
- You can soon securely unlock smartphone with your “body sweat”
- VMware Patches Vulnerabilities in vCenter Server
- Adobe, Microsoft Patch Critical Cracks
- Google researcher finds 79 Linux USB vulnerabilities
- Android beats iOS and Windows as least-secure mobile OS, Nokia report finds
- Forever 21 Warns Shoppers of Payment Card Breach at Some Stores
- Hackers mimicking little kids can fool voice recognition systems
- Amazon Echo and Google Home Devices Vulnerable to BlueBorne Attack
- Locking Down Your Website Scripts with CSP, Hashes, Nonces and Report URI
- Amazon key flaw could let rogue deliverymen disable your camera
- New free Quad9 DNS service has built-in security, privacy settings to protect internet users

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us