kindred

Security Newsletter

21 October 2019

Subscribe to this newsletter

Samsung Galaxy S10 Fingerprint Reader Defeated by Silicone Case

A couple in the UK experienced a weird bug on their Samsung Galaxy S10 that allows bypassing the fingerprint reader to unlock the phone regardless of the biometric data registered in the device.

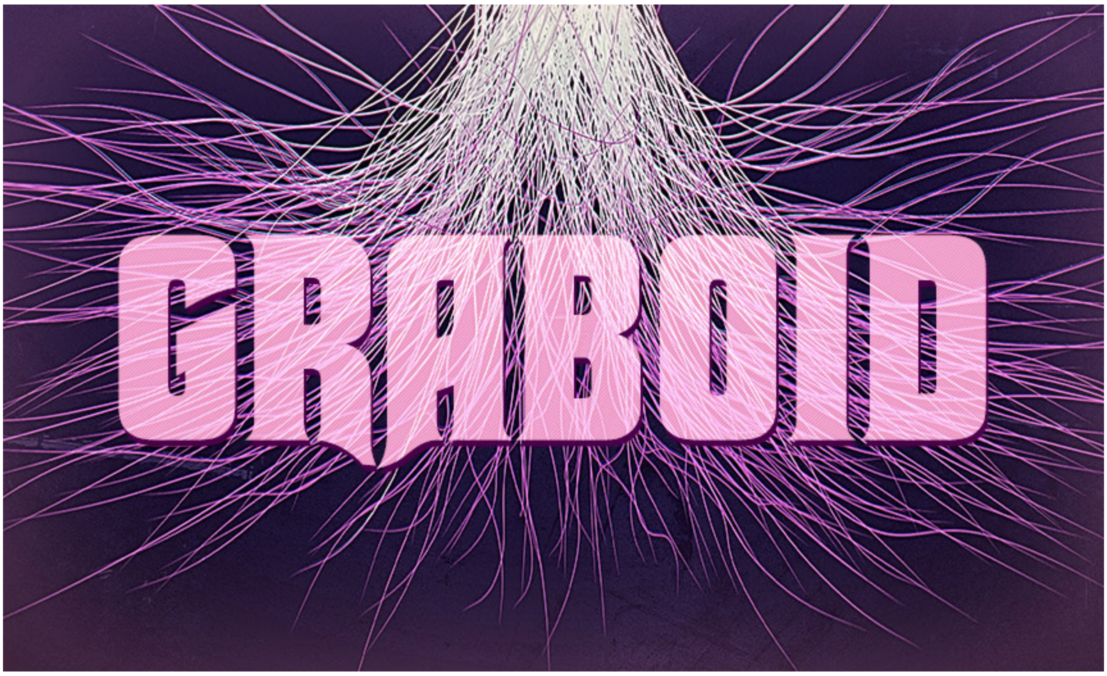
Lisa got the phone as a gift from her husband and decided to put it in a protective case. She soon discovered that even if only her own fingerprint was registered in the biometric settings of the device, the phone unlocked no matter what finger was used for the process. The culprit seems to be the the silicone case, which somehow confuses Samsung Galaxy S10's fingerprint reader and allows any fingerprint to unlock the device.

Both Galaxy S10 and S10+ create a 3D map of the fingerprint using ultrasounds, with the reader being embedded under the display. These devices were the first phones to use this technology for fingerprint scanning. Also worrying is the fact that many banking apps adopted biometric authentication, so bypassing the fingerprint reader on a phone also allows executing financial operations. Following media reports that the fingerprint reader in Samsung Galaxy S10 phones unlocks the device when scanning unregistered fingerprints through a silicone case, the South Korean company informs that it will release a patch to correct the problem.

Read More on BleepingComputer

Samsung to Patch Fingerprint Scanner

'Graboid' Cryptojacking Worm Spreads Through Containers



Attackers are using Docker containers to spread a cryptojacking worm in a campaign dubbed "Graboid," according to researchers at Palo Alto Network's Unit 42 threat research unit. Although the researchers describe the campaign as "relatively inept," they says it has the potential to become much more dangerous.

This is the first time the researchers have seen a cryptojacking worm spread through containers in the Docker Engine (Community Edition). While the worm isn't sophisticated in its tactics, techniques or procedures, it can be repurposed by the command-and-control server to run ransomware or other malware, the researchers warn.

Researchers say that organizations can take several steps to protect containers from attack. Those include ensuring that Docker daemons are not exposed to the internet unless they have a proper authentication method, using Unix socket to communicate with the daemon locally or Secure Shell to connect to a remote daemon, and using firewalls to whitelist incoming traffic.

Read More BankInfoSecurity

What Your Personal Information is Worth to Cybercriminals

Cybercriminals have multiple markets to get illicit goods and prices on these underground forums are likely driven by supply and demand, just like in the legal economy. Offerings found on deep and dark web (DDW) markets include anything that can be monetized in one way or another. Common goods cover any financial information that can be used for bank fraud.

A typical assortment of products and services comprises personally-identifiable information, payment card data, credentials, access to compromised systems, distributed denial-of-service, forged documents, credentials, and access to compromised services. Full packages of data that can be used to steal a US victim's identity sell for $4-$10, the researchers say. These are called 'fullz' and include at least the name, Social Security number, date of birth, and account numbers.

Flashpoint estimates "with a moderate degree of confidence in 2019 that the price of cards in card shops likely often ranges between $2 and $20 USD" but it may go as high as $200 in some cases. Although the prices above seem low, one must consider that the seller expects to deliver them in bulk. For instance, someone is offering a huge database of 90 million Brazilian citizens, while others provide entire collections of credentials, suitable for account takeover attacks via credential stuffing.

Read More on BleepingComputer

More #News

- Guarding against supply chain attacks—Part 1: The big picture
- Microsoft Adds Azure AD Sign-In History to Detect Unusual Activity
- Yubico security keys can now be used to log into Windows computers
- Zappos data breach settlement: users get 10% store discount, lawyers get $1.6m
- Hundreds of Fake Election Domains Target Democrats, Republicans
- 500+ Million UC Browser Android Users Exposed to MiTM Attacks. Again.
- Facebook Now Pays Hackers for Reporting Security Bugs in 3rd-Party Apps
- Cracking the Passwords of Early Internet Pioneers
- Facebook's Libra cryptocurrency loses all but one payment company
- WAV audio files are now being used to hide malicious code

- WAV audio files are now being used to hide malicious code
- Firefox Blocks Inline and Eval JavaScript on Internal Pages to Prevent Injection Attacks
- M6, one of France's biggest TV channels, hit by ransomware
- Linux SUDO Bug Lets You Run Commands as Root, Most Installs Unaffected
- Microsoft Defender 'Tamper Protection' reaches general availability
- FBI urges businesses to use biometric factors to mitigate multi-factor authentication risk
- SIM Cards in 29 Countries Vulnerable to Remote Simjacker Attacks
- Microsoft and NIST partner to create enterprise patching guide
- Microsoft Improves Azure Active Directory Security with New Roles
- NordVPN was Hacked. Here's What We Know

#Patch Time!

- Adobe Fixes 45 Critical Vulnerabilities in Acrobat and Reader
- WordPress 5.2.4 Patches Six Vulnerabilities
- Adobe Releases Out-of-Band Security Patches for 82 Flaws in Various Products
- Critical Flaw in Sophos Cyberoam Appliances Allows Remote Code Execution
- Nitro PDF Pro to Get Micropatches for 7 Potential RCE Bugs
- Google Patches 8 Vulnerabilities in Chrome 77

#Tech and #Tools

- A Thorough Introduction to PASETO (JWT secure alternative)
- YARA v3.11.0
- Phishing e-mail spoofing SPF-enabled domain
- Patching Android apps: what could possibly go wrong
- CSS Injection Primitives
- Weaponizing and gamifying ai for wifi hacking: presenting pwnagotchi 1.0.0
- DOMDig: DOM XSS scanner for Single Page Applications
- Ahh shhgit!
- XML External Entity(XXE)
- JA3/S Signatures and How to Avoid Them
- RDP Honeypotting
- Analysis of Two Newly Patched Kubernetes Vulnerabilities
- Securing Docker Containers
- Blowhole: Docker auditing and enumeration script.
- Fun with Amazon S3— Leaks and bucket takeover attack
- Hunting for Suspicious LDAP Activity with SilkETW and Yara
- Blue Hands On Bloodhound
- Active Directory Security: Beyond the Easy Button
- Hunting for Anomalous Usage of MSBuild and Covenant
- SANS Blue Team Wiki
- Assessing the effectiveness of a new security data source: Windows Defender Exploit Guard
- Red Team Tactics: Active Directory Recon using ADSI and Reflective DLLs
- Office 365 network attacks - Gaining access to emails and files via an insecure Reply

- Office 365 network attacks – Gaining access to emails and files via an insecure Reply URL

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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