Name: Legion of redwind01
University ID: CLASSIFIED
Thomas Edison State University
Spring board
Section no.: X.X.X
2021.05.20.16.06.00.759
[X]
[ ]

6.5.1 Mini-Project 14: Security Incident Research (Mobile)

A few of the concepts here are not listed in the file “6.4.3 NIST SP 800-147, BIOS Protection Guidelines“

Execute Disable/Enhanced Virus Protection
Intel Trusted Execution Technology (TXT)
Wake On LAN

EMAIL:
TO:
SUBJECT:
BODY:

1. The link below, from Kaspersky Lab's official blog, SecureList, discusses the

how the trojan gets installed,

The app (either APK or zip file) is Installed by users while it is disguised as a valid desirable application.

what it does upon execution,

uses Accessibility Mode to gain persistence, disable manual uninstallation and allow the banking trojan to capture data, manipulate screen content and provide full remote control to the fraudster

it tries to detect common emulators,
checks for a debugger attached to the process and the manifest file
checks for a debuggable flag.
If present, the malware terminates itself.
Newer versions move the emulator names to an encrypted configuration file.

The malware also blocks the user from uninstalling it, restarting or shutting down the device.

how it hides itself, and

the app pretends to be Google Defender, Google Docs, WhatsApp Updater, etc.

Ghimob hides the icon from the app drawer

what information it steals.

phone model,
whether it has a screen lock activated
list of all installed apps that the malware has as a target including version numbers.
Ghimob spies on 153 mobile apps, mainly from banks, fintechs, cryptocurrencies and exchanges.
Ghimob sends accessibility-related information from the current active window

2. Answer the following questions regarding the behavior of the trojan:

How does Ghimob bypass the security measures implemented by financial institutions?

once infection is completed, the hacker can access the infected device remotely, completing the fraudulent transaction with the victim's smartphone, so as to avoid machine identification, security measures implemented by financial institutions and all their antifraud behavioral systems

if the user has a screen lock pattern in place, Ghimob is able to record it and later replay it to unlock the device.

Why does the trojan abuse Accessibility Mode?

Ghimob sends accessibility-related information from the current active window

How are victims lured into installing the malicious file?

Victims are lured in by an email that is written as if it were from a creditor and provides a link where the recipient could view more information

What happens once the infection is completed?

Ghimob monitors the Portuguese words for balance, investment, lending, and statement. Ghimob sends accessibility-related information from the currently active window

3. What can be done to mitigate the risk of infection?

Do not download anything from untrusted sites
If an app is needed it should only be download from trusted application downloaders.

$

$

$

$

$

$

$

$

$

$

$

$

$

TOOLS
†
?
¬ ⋀ ⋁ ⟶ ⇒ ↔ ⇔ ⊕ ≡ ≠ ∅ ⊂ ⊃ ∀ ∃ ⊆ ⊇ ∵ ∴

¬!~	/not
⋀ &&	/and
⋁	/or
⟶ => ⇒	/ifthen or /implies
↔ ⇔	/congruence
	Must agrea no matter right or wrong
⊕ ⩒	/xor
	Only one true value
≡	/iden or /identical or /identical to
≠	/xi/
∅	/phi /empty /emptyset /empty set
∪	/union
∩	/intersection
⊂	/subset
⊃	
∀	/forall
∃	/exists /there are
	existential quantifier
	“there exists” or “for some” or
	“There is a case in which”
⊆	
⊇	
∴	/therefore
∵	/because
≤	/le
≥	/ge
≠	/ne

ANN (Artificial Neural Network)

First Order Logic:
First-order logic is symbolized reasoning in which a sentence is broken into subject and predicate. A sentence in first-order logic is written as P(x), where P predicate and x is subject.

($\exists^1$): There exists exactly one
Parent(p,q) : P is parent of q

parent “p” of “q”
parent “p” has child “q”

Female(p) :p is female

Everyone is loved by someone.

$\forall$ y	For all ys [and]
$\exists$ x	there exists a case in which “x”
love(y, x)	all “y”s are loved by an “x”

$\forall$ y $\exists$ x love(y, x)

https://en.wikipedia.org/wiki/List_of_mathematical_symbols

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus. Vivamus elementum semper nisi. Aenean vulputate eleifend tellus. Aenean leo ligula, porttitor eu, consequat vitae, eleifend ac, enim. Aliquam lorem ante, dapibus in, viverra quis, feugiat a,