



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

Cyber Espionage Service Advertised

Moderately credible threat actor “CINT” advertised a cyber espionage service on both the English language Dark Web forum “CryptBB” and the predominantly Russian language Dark Web forum “XSS.” The actor claims that the service offers business owners a competitive advantage by stealing confidential data from rival companies, including:

- Research and development
- Financial documents
- Marketing and business plans
- Personally identifiable information (PII) of employees

The actor specified that the service does not use malware to compromise target networks, indicating it would likely be more difficult for enterprise defenders to detect a breach.

ZeroFox assesses the service likely leverages insiders, or some other method designed to streamline the exploitation of corporate Human Resources departments at scale, as the actor claimed that their method was very specialized, leveraging a large network to exfiltrate data.

Our researchers cannot rule out the possibility that this is a scam, since there are no vouches for the service and the actor is charging peers to test it.

Original post from threat actor "CINT" advertising a cyber espionage service

Cyber Espionage Service Advertised (Cont.)

Cyber Espionage Service



CINT •
Junior
Member

Posts: 10
Joined: Sep 2022
Reputation: 2

#1

01-03-2023, 04:17 PM

Get a competitive edge in the industry: obtain advantageous confidential information such a research and development, financial information, marketing and business strategies, personnel management, and much more.

Thanks to our large network and capabilities we've helped countless companies increase their revenue by tens of millions of dollars (estimates based on industry and discovered competitors data). All for a negligible initial investment.

Differently to other organizations that provide similar services, the target company will not notice our activity or any indicator of compromise. We do not install ransomware or any other type of malware for our own profit. Everything we do, we do for our clients, in complete secrecy.

As our service is very specialized we do not disclose the process from start to finish, but you can know more for free by contacting us. We will answer any question you have, and estimate a price and time for your target if you wish so.

email: evilarchitect@swissmail.be

Malware Loader Disguised As Legitimate Mobile App On Google Play Store

Untested threat actor “Marx” advertised a malware loader embedded in a legitimate financial services application on the Google Play Store, on the predominantly Russian language Dark Web forum “Exploit.” A threat actor could leverage this loader to compromise Android devices with banking malware, like “Cerberus,” “Vultur,” or “GodFather.” This would almost certainly lead to an increase in cyber-attacks against the customers of various financial institutions, since these malware strains are specifically designed to steal the full banking information of victims.

The actor charged \$3,000 USD per week to use the loader.

ZeroFox researchers assess the actor is likely credible based on the fact that they agreed to use an escrow service, which would require the actor to use a forum admin or middleman to complete the transaction.



Android loader in Playstore

By Marx, Saturday at 01:28 AM in [Software] - malware, exploits, bundles, crypts

Marx

megabyte

●●●



Paid registration

● 0

55 posts

Joined

07/30/19 (ID: 94687)

Activity

вирусология / malware

Posted Saturday at 01:28 AM

I offer android loader in playstore finance theme Ecrow accepted price 3k for 7 days pm me for detail

+

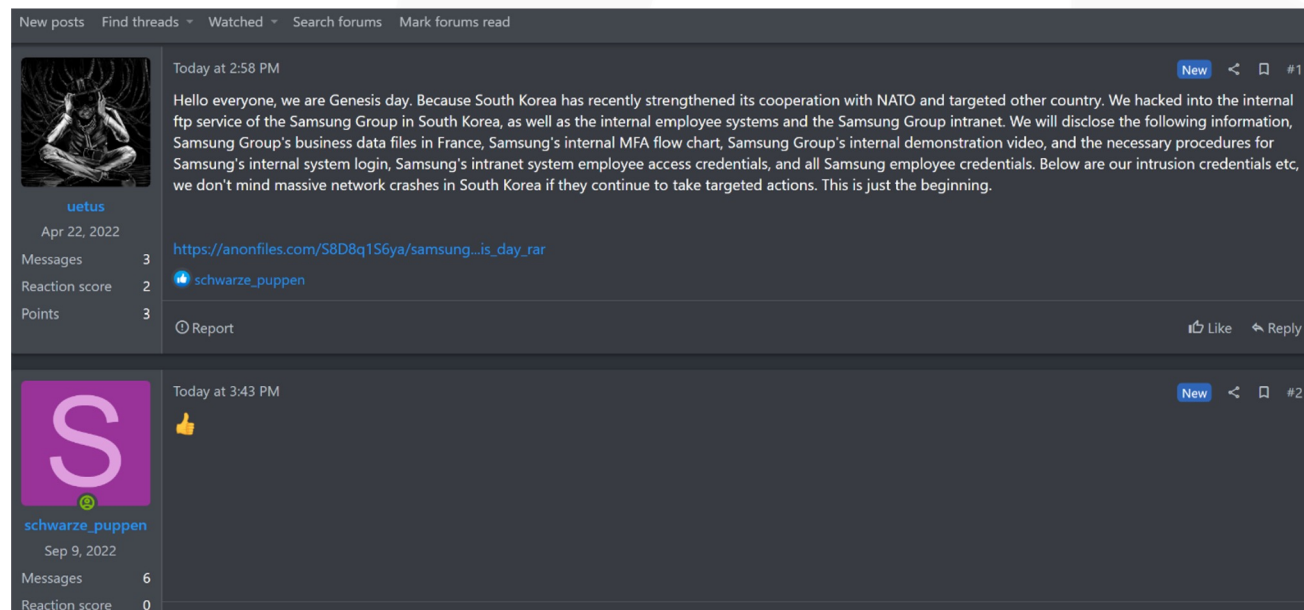
Quote

4

Alleged Data Breach At Samsung Announced

Moderately credible threat actor “uetus” announced an alleged data breach impacting Samsung, on the predominantly Russian language Dark Web forum “RAMP.” The actor claims that their team, dubbed “Genesis,” compromised the company’s file sharing server in response to South Korea’s increasing cooperation with NATO. The alleged leak contains employee account credentials and various documents and videos highlighting internal operational security (OPSEC) procedures, including multi-factor authentication details.

ZeroFox researchers assess that the “Genesis” group is likely working with an insider at Samsung who is politically motivated, since the actor condemned alleged attacks by South Korea against an unnamed country and threatened to disrupt South Korean networks if these attacks persisted.



Actor Looking For Compromised Business Accounts For Phishing Scam

New and untested threat actor “jaba42” is looking for peers with compromised business email accounts for a phishing scam, on the predominantly Russian language Deep Web forum “Club2Crd.” The actor said they would use the email accounts to launch phishing campaigns against other employees at the target organizations. This would make the phishing emails seem more legitimate to victims, as the messages would be coming from legitimate email servers. The emails would have weaponized invoice documents attached, which are designed to compromise a victim’s device and exfiltrate sensitive data.

The actor said that they would split the profits from any successful phishing attempts, indicating the actor likely intends to cash out stolen funds from a victim’s banking or cryptocurrency accounts.

