New Unix rootkit used to steal ATM banking data

bleepingcomputer.com/news/security/new-unix-rootkit-used-to-steal-atm-banking-data/

Bill Toulas

By
Bill Toulas

- March 17, 2022
- 06:23 PM
- 0

Threat analysts following the activity of LightBasin, a financially motivated group of hackers, report the discovery of a previously unknown Unix rootkit that is used to steal ATM banking data and conduct fraudulent transactions.

The particular group of adversaries has been recently observed targeting telecom companies with custom implants, while back in 2020, they were spotted compromising managed service providers and victimizing their clients.

In a new report by Mandiant, researchers present further evidence of LightBasin activity, focusing on bank card fraud and the compromise of crucial systems.

Tapping into your banking data

LightBasin's new rootkit is a Unix kernel module named "Caketap" that is deployed on servers running the Oracle Solaris operating system.

When loaded, Caketap hides network connections, processes, and files while installing several hooks into system functions to receive remote commands and configurations.

The commands observed by the analysts are the following:

- Add the CAKETAP module back to the loaded modules list
- Change the signal string for the getdents64 hook
- Add a network filter (format p)
- Remove a network filter
- Set the current thread TTY to not to be filtered by the getdents64 hook
- Set all TTYs to be filtered by the getdents64 hook
- Displays the current configuration

The ultimate goal of Caketap is to intercept banking card and PIN verification data from breached ATM switch servers and then use the stolen data to facilitate unauthorized transactions.

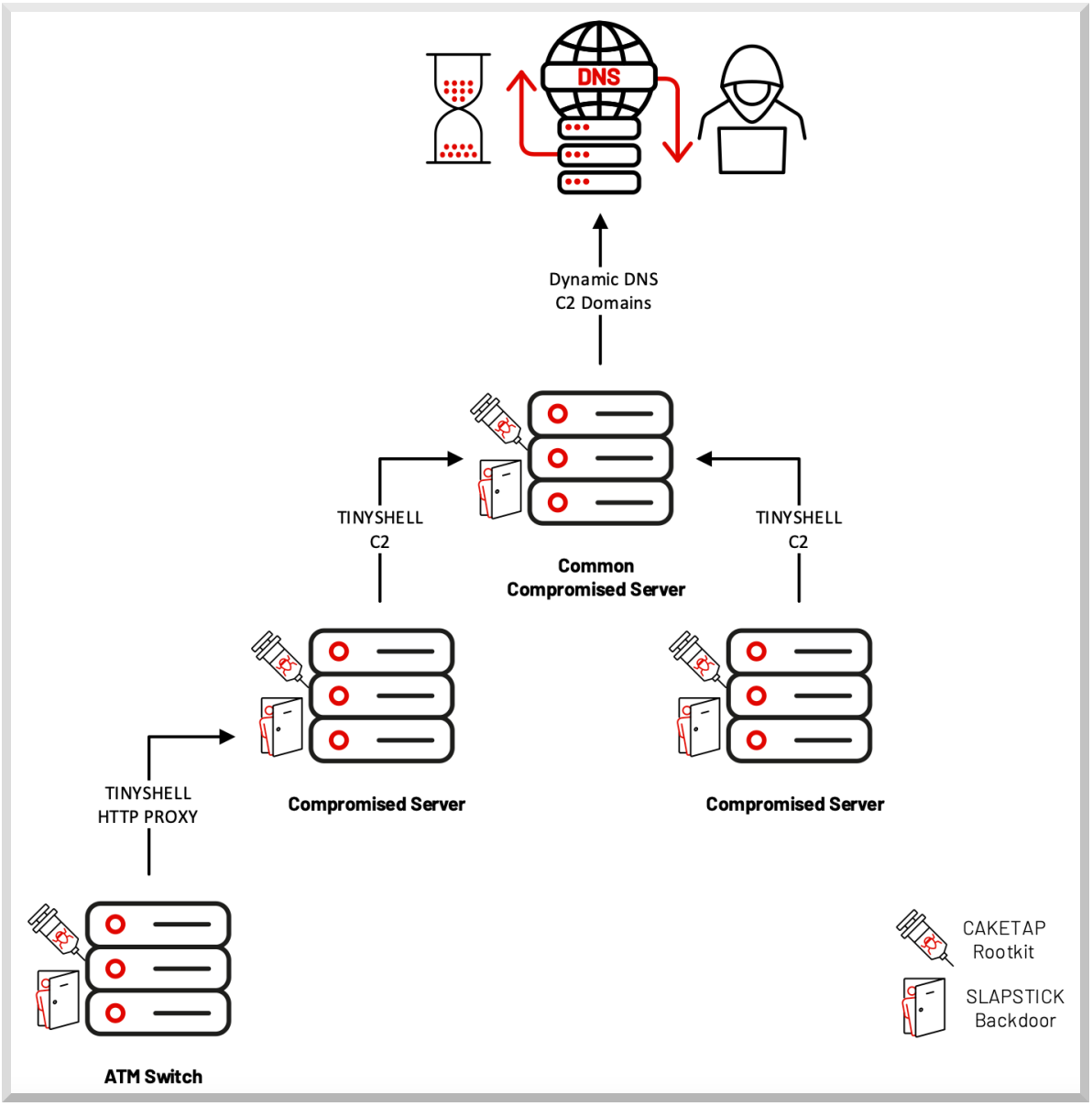
The messages intercepted by Caketap are destined for the Payment Hardware Security Module (HSM), a tamper-resistant hardware device used in the banking industry for generating, managing, and validating cryptographic keys for PINs, magnetic stripes, and EMV chips.

Caketap manipulates the card verification messages to disrupt the process, stops those that match fraudulent bank cards, and generates a valid response instead.

In a second phase, it saves valid messages that match non-fraudulent PANs (Primary Account Numbers) internally and sends them to the HSM so that routine customer transactions aren't affected and the implant operations remain stealthy.

“We believe that CAKETAP was leveraged by UNC2891 (LightBasin) as part of a larger operation to successfully use fraudulent bank cards to perform unauthorized cash withdrawals from ATM terminals at several banks,” explains Mandiant’s report.

Other tools linked to the actor in previous attacks include Slapstick, Tinyshell, Steelhound, Steelcorgi, Wingjook, Wingcrack, Binbash, Wiperight, and the Mignogcleaner, all of which Mandiant confirmed as still deployed in LightBasin attacks.



LightBasin uses Caketap, Slapstick, and Tinyshell in every step *(Mandiant)*

Sophisticated targeting

LightBasin is a highly skillful threat actor that takes advantage of relaxed security in mission-critical Unix and Linux systems that are often treated as intrinsically secure or largely ignored due to their obscurity.

This is precisely where adversaries like LightBasic thrive, and Mandiant expects them to continue to capitalize on the same operational strategy.

As for attribution, the analysts spotted some overlaps with the UNC1945 threat cluster but don't have any concrete links to draw safe conclusions on that front yet.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

National bank hit by ransomware trolls hackers with dick pics

Iranian hackers exposed in a highly targeted espionage campaign

Bitter cyberspies target South Asian govts with new malware

Hackers display “blood is on your hands" on Russian TV, take down RuTube

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.