KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Threat actors using DarkTortilla RAT to evade detections

Tracker ID: TN0829 **Date:** 25/Aug/22 **Category:** Malware **Industry:** All **Region**: All

Background

Several threat actors are utilizing a clever, elusive crypter to spread a variety of information stealers and remote-access Trojans (RATs). One of them, the "DarkTortilla" crypter, is pervasive and persistent. It has many features that are intended to help it evade anti-malware and forensics technologies. The.NET-based crypter can be designed to deliver a variety of malicious payloads and may be used to infiltrate a victim's machine with illicit software. Additionally, it can deceive users and sandboxes into thinking it is harmless.

DarkTortilla was discovered for the first time in October 2021, when a threat actor used the Microsoft Exchange remote code execution vulnerability (CVE-2021-34473) to run malicious PowerShell inside client environments. The attack chain resulted in the download and execution of the.NET malware DarkTortilla. Threat actors have previously used DarkTortilla to deliver malware such as Remcos, BitRat, FormBook, WarzoneRat, Snake Keylogger, LokiBot, QuasarRat, NetWire, and DCRat. The crypter has also been used in targeted assaults to deliver payloads such as Metaspolit and Cobalt Strike. It has most recently been used to propagate malware such as the information-stealing RedLine and the RATs AgentTesla, NanoCore, and AsyncRat.

One of DarkTortilla's various tactics is a customized message box stating that the malware is a legitimate application, that the execution failed, or that the software is contaminated. Once again, the goal is to trick users into thinking that malware running on their PC is benign. Threat actors have been spotted in a few cases using DarkTortilla to store add-ons on disc but not run them afterwards. To propagate DarkTortilla, attackers have used spam emails with file attachments such as.ISO,.ZIP,.PDF,.docx, and.IMG.

DarkTortilla exhibited that it migrates execution to the Windows %TEMP% directory on first execution. From the attacker's perspective, one advantage of doing so is that it allows DarkTortilla to hide on an infected system. Second, if the %Delay% configuration element is defined within the DarkTortilla configuration, the time between when DarkTortilla is started and when the primary payload is executed grows exponentially. An attacker, for example, can make the malware's main payload run after the DarkTortilla executable has been running for a few minutes by making a few parameter changes.

DarkTortilla's loader, the only element of the malware that interacts with the file system, has a limited set of characteristics, making it difficult to detect. Its primary purpose is to retrieve, decode, and load the core processor, stored in the initial loader's resources as encrypted data. The code varies between samples and is generic, depending on the obfuscation techniques used.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Threat actors using DarkTortilla RAT to evade detections

Tracker ID: TN0829 **Date:** 25/Aug/22 **Category:** Malware **Industry:** All **Region**: All

DarkTortilla is dangerous owing to its great degree of configuration flexibility and extensive anti-analysis and anti-tampering measures, which make detection and analysis extremely difficult. The malware, for example, conceals its code using open-source tools like as DeepSea and ConfuserEX, and its main payload is executed fully in memory.

From January to May 2021, an average of 93 distinct DarkTortilla samples were posted to VirusTotal each week. More than 10,000 different DarkTortilla samples have been detected since malware tracking began. It is often overlooked because of its primary payload. But it can avoid detection, is highly configurable, and spreads a wide range of well-known and efficient malware. Given its power and pervasive existence, it poses a severe concern.

MITRE ATT&CK Tactics

Initial Access, Execution, Persistent, and Defense Evasion.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- To reduce the risk of infection and avoid using pirated software, never use software product activators, illegal key generators, or cracked files that claim to provide you with free access to premium programs.
- Avoid clicking on software update notifications and links in emails or pop-up windows.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Block spoofed emails, spam, and emails containing malicious attachments.
- Ensure employees are aware of the ongoing phishing campaigns and techniques.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Threat actors using DarkTortilla RAT to evade detections

Tracker ID: TN0829 **Date:** 25/Aug/22 **Category:** Malware **Industry:** All **Region**: All

References

- COUNTER THREAT UNIT RESEARCH TEAM, DarkTortilla Malware Analysis, SecureWorks, 17th August 2022, External Link (secureworks.com).
- Jai Vijayan, 'DarkTortilla' Malware Wraps in Sophistication for High-Volume RAT Infections, Dark Reading , 18th August 2022, External Link (darkreading.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

*

Hash MD5	Hash SHA256	URL
59295e810bbdbfd64b8c41316ea13cae	981aa83b2d33cca994021197237ac5ee3ad3402f7d25f04f4e76985f4ec8744c	https://pastebin.pl/view/raw/60b6b03b
84872b60072011eab8940f3b49bdb582	5e03556be992d23088a3c49d24c45b1c21cd275bffb4e536348e8128d50374b6	
2d74df3ce221f6ff48d20bac158a3e78	4f15b28c91fa0e8d0dd9e86481bad04fa34fcaf564d08de7c4c0c513fc6e122d	
827258f907c5087f498c413d28e2203e	60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145	
c37aae0ff565a2e44f144f837b750279	55d7d9bd9d4a511417033b6c14ce93f962d6a6e6c6414f0cb7e455baee1d3ab7	
93fe6600c51014d7d6c2afedf8398f92	a0b96236bfd79d2ebeadb8e3deb9448af3ec8edd1ea9672b7ad4793934bb4c47	
6e91ad0972e104a277505104abe39d1e	45ef054bca2ae4d67e6623bf28ff75e5d178924602674c654e1b569aa74601cd	
cd49f7c3c4e82dee128eedea9879bc33	b3754c6ecc445e9a3b37c5ebe68adb9630ca4aa89a8e8515468f39ae8131f141	
851816aa8cf45ba769f0d9420acfb3e5	0a5dc3b6669cf31e8536c59fe1315918eb4ecfd87998445e2eeb8fed64bd2f2c	
f44695a8febb2a35576a59fa984629d2	083acce46cb8cf35e37c778d1f4aee6814bca72d2874b793a47f9823f51df0fe	
8d8c551dd572a1dc158de239b37eaa9a	53b3b37b7d1e40c80fcda2c424cd837379ac2ce93023de6c22ba3e2d94679671	
0f89a2015ed9c1be5522e27c00276e52	5be86cfca25e295f88b5aab42a6f604d2f1bb97f3c73b01df664c137908e2ec4	
0e362e7005823d0bec3719b902ed6d62	93dd1202697dbaed9ef4f4707f2628212bf13aad096de29c14924b1dae1d6d5b	
	2d0dc6216f613ac7551a7e70a798c22aee8eb9819428b1357e2b8c73bef905ad	