LEET MX

A SURVEY ON LEETMX: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

LeetMX is a cyber campaign that originated from Mexico and had been targeting since November 2016. Their motivation seemed to be around Information Theft and Cyber Espionage. LeetMX's infrastructure included 27 different hosts and domains used for malware delivery or as C2 Server. Hundreds of malware samples have been used, most are Remote Access Trojans and keyloggers. Interestingly, the attackers camouflage one of their delivery domains by redirecting visitors to El Universal, a major Mexican newspaper.

II. TARGET SECTORS

Countries like Argentina, Costa Rica, El Salvador, Guatemala, Mexico, and the USA.

III. OPERATIONS

- This Cyber-Operation focused on targets in Mexico, El Salvador, and other countries in Latin America, such as Guatemala, Argentina, and Costa Rica as well as the USA. They would deliver malicious Office documents to targets. These documents contain macros that run PowerShell, which downloads and run various payloads from domains and hosts controlled by the attackers. Multiple parts of the malicious infrastructure indicate that the attackers are based in Mexico. More than 550 samples used in this campaign are available on VirusTotal. Most of them are Xtreme RAT variants and iSpy Keylogger.

AX1AL

IV. IOC

MD5

- 6ad3b410e12fd563013cec23d4dc2119
- fe3f64525f9f40387d4542986c48aa60
- db964aba419a85e69d43d17075ef9c95
- f8e1ab2b757a28dfd6e5e70ba37137a2
- 6ff889576b72c8a31cd7de98c4283297
- 830baa3bd79c8e5a8aad03bd7791d7b1
- a40053b2d40f7a27cadd2cc84af61c72
- 48dee0033baf8d606b2fbb649a6e4b71
- 3918ff2717247c2de90ded7775720d85
- 3c3a4cf861dd803a927d1fb436e26ae4

C2

1. c0pywins.is-not-certified[.]com
2. casillas.hicam[.]net
3. casillas45.hopto[.]org
4. casillasmx.chickenkiller[.]com
5. cloudrsaservicesdriveoffic[.]com
6. cloudsfullversionooficcekey[.]com
7. dryversdocumentofficescloud[.]com
8. dryversdocumentsandcustom[.]com
9. dryversdocumentsandcustomer[.]com
10. dryversdocumentsandcustoms[.]com
11. dryversdocumentsandcustomsoft[.]com

V. REFERENCES

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=leetMX&n=1
- https://www.clearskysec.com/leetmx/
- https://docs.google.com/spreadsheets/d/1HrxjP1gpIjBJ51VTZa5yGmwVRnzsCc1PkYPkRx0-V5M/edit?usp=sharing