Jun 19 2023

NETMANAGEIT

Intelligence Report

Xneelo Users Targeted in a Multi-stage Phishing Attack

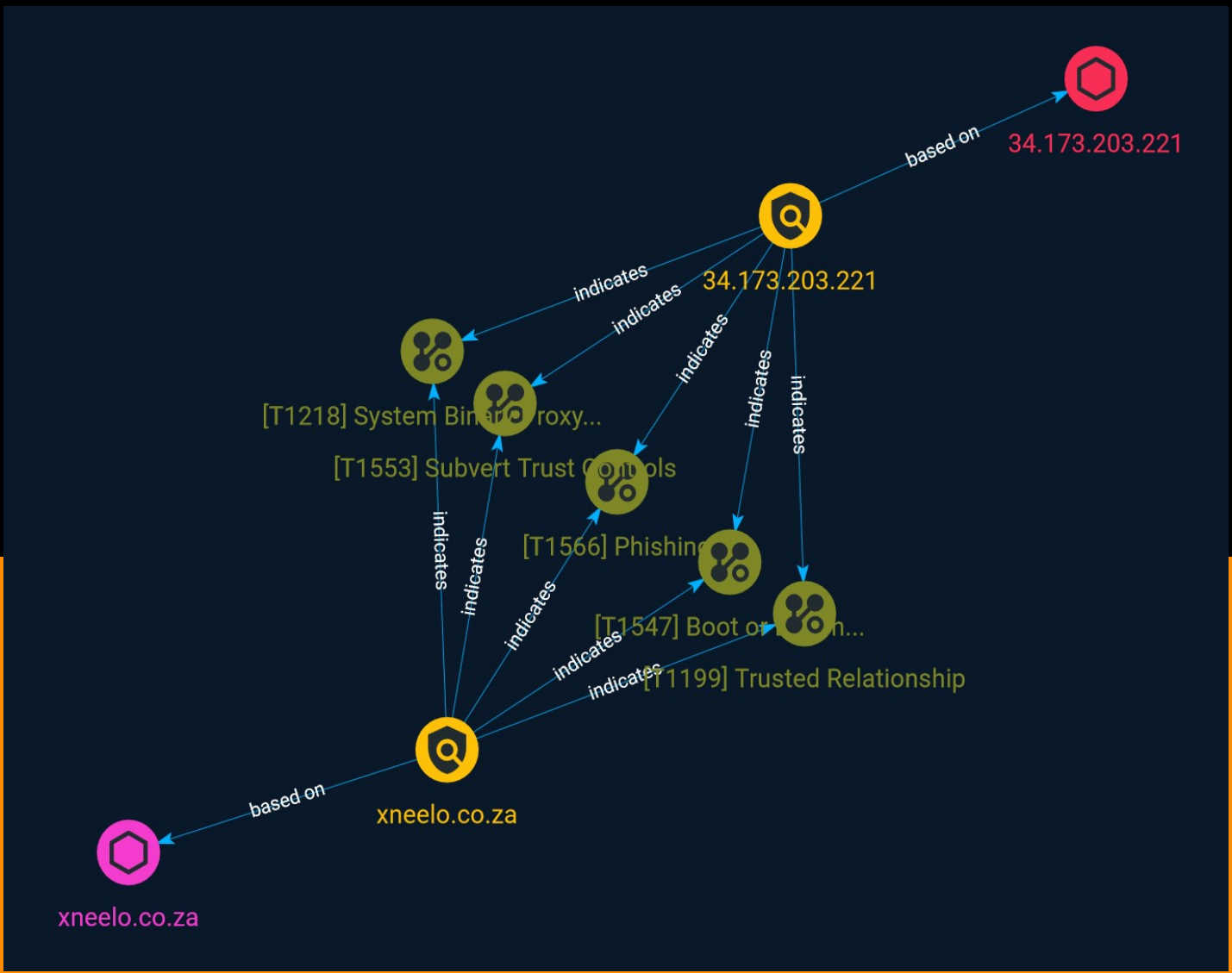

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers discovered a multi-stage phishing campaign targeting customers from Xneelo, a South African web hosting provider who supports over 500,000 customers.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may

attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Trusted Relationship

ID

T1199

Description

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used. (Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Indicator

Name

34.173.203.221

Description

ISP: Google LLC **OS:** None ---------- Hostnames: - totalsim.us - 221.203.173.34.bc.googleusercontent.com ---------- Domains: - totalsim.us - googleusercontent.com ---------- Services: **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 13 Jun 2023 09:11:47 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Keep-Alive: timeout=20 Location: https://klingenstein.org ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 16 Jun 2023 00:54:58 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 319753 Connection: keep-alive Keep-Alive: timeout=20 Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Link: ; rel="https://api.w.org/" Link: ; rel="alternate"; type="application/json" Link: ; rel=shortlink X-Powered-By: WP Engine X-Cacheable: SHORT Vary: Accept-Encoding,Cookie Cache-Control: max-age=600, must-revalidate Accept-Ranges: bytes X-Cache: HIT: 2 X-Cache-Group: normal ``` HEARTBLEED: 2023/06/16 00:55:05 34.173.203.221:443 - SAFE ---------- **2222:** ``` SSH-2.0-mod_sftp Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC4vpOtSV41F5hVTZzJKwqV6gsU4lz7kGCSkzLWltDeTBAc9V9cy1l5R+yiPcJThVCW4Lc36xaPxGE+Z24kfOhmNDXgFm7jMky+FNSoXxo2szXWqq0yQJvPR83oSVAvshgajZ5tCD0fEV7lomQ7dj5qwySyI7FssYAN9MGkjUdE36YXmoDzxdr8XtsaOL5LBD3idRBHkxjTZv8PsRkBIDCXhF6YmYFJZRzz/ZQXx+D90qjWptv6xzmg7sXoDQSzkpPvyCRB5p6bKJ3RBYNXh/tYceaV/qIWBtIq/TtU+L8G7h9R08Rnj2m60/Uo77Ns8bPHkjtwAN4wVH7U4gktSAVR Fingerprint: 16:19:52:1b:79:08:5b:ea:f6:7d:7e:25:40:aa:18:02 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group18-sha512 diffie-hellman-group16-sha512 diffie-hellman-group14-sha256 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 rsa1024-sha1 ext-info-s Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr MAC

Algorithms: hmac-sha2-256 hmac-sha2-512 Compression Algorithms: zlib@openssh.com zlib none ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '34.173.203.221']

Name

xneelo.co.za

Pattern Type

stix

Pattern

[domain-name:value = 'xneelo.co.za']

Domain-Name

Value
xneelo.co.za

IPv4-Addr

Value
34.173.203.221

External References

- https://cofense.com/blog/xneelo-users-targeted-in-a-multi-stage-phishing-attack/
- https://otx.alienvault.com/pulse/649077a2372e7efdf162ac44