Jun 22 2023

NETMANAGEIT

Intelligence Report

Why Malware Crypting Services Deserve More Scrutiny

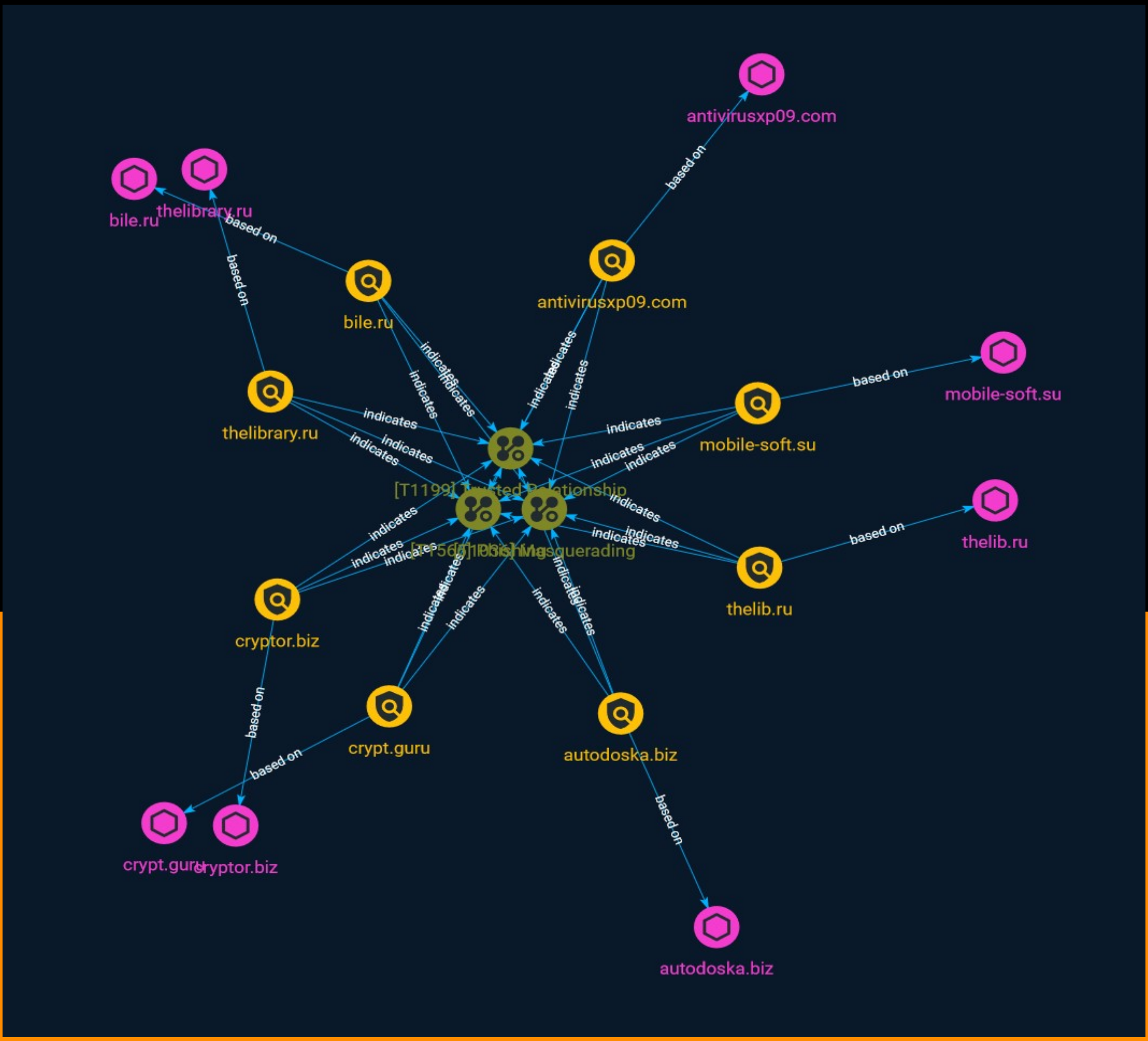

Table of contents

Overview

Entities

Observables

External References

Overview

Description

KrebsonSecurity explores the history and identity behind Cryptor[.]biz, a long-running crypting service that is trusted by some of the biggest names in cybercrime.

Confidence

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

15 / 100

Attack-Pattern

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

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

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)

Indicator

Name
autodoska.biz
Pattern Type
stix
Pattern
[domain-name:value = 'autodoska.biz']
Name
thelibrary.ru
Pattern Type
stix
Pattern
[domain-name:value = 'thelibrary.ru']
Name
mobile-soft.su

Pattern Type
stix
Pattern
[domain-name:value = 'mobile-soft.su']
Name
crypt.guru
Pattern Type
stix
Pattern
[domain-name:value = 'crypt.guru']
Name
bile.ru
Pattern Type
stix
Pattern
[domain-name:value = 'bile.ru']
Name
thelib.ru

Pattern Type

stix

Pattern

[domain-name:value = 'thelib.ru']

Name

cryptor.biz

Pattern Type

stix

Pattern

[domain-name:value = 'cryptor.biz']

Name

antivirusxp09.com

Pattern Type

stix

Pattern

[domain-name:value = 'antivirusxp09.com']

Domain-Name

Value
cryptor.biz
bile.ru
mobile-soft.su
autodoska.biz
thelib.ru
antivirusxp09.com
crypt.guru
thelibrary.ru

External References

- https://otx.alienvault.com/pulse/64944c08e39f6f341f7add45
- https://krebsonsecurity.com/2023/06/why-malware-crypting-services-deserve-more-scrutiny/