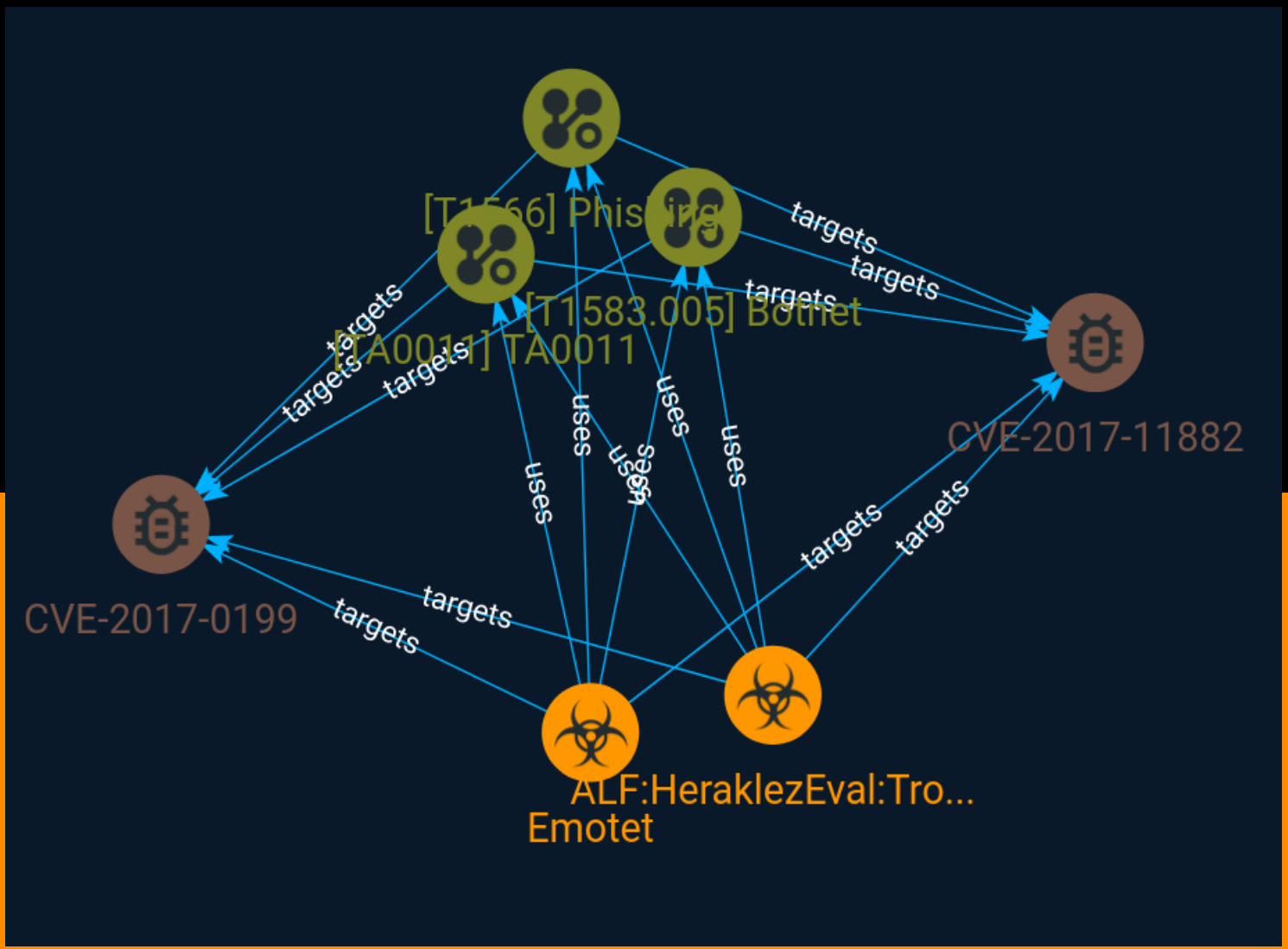
Aug 03 2023

NETMANAGEIT

# Intelligence Report

# What's happening in the world of crimeware: Emotet, DarkGate and LokiBot



# Table of contents

## Overview



## Entities



## External References

# Overview

## Description

The malware landscape keeps evolving. New families are born, while others disappear. Some families are short-lived, while others remain active for quite a long time. In order to follow this evolution, we rely both on samples that we detect and our monitoring efforts, which cover botnets and underground forums.

## Confidence

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

15 / 100

# Malware

| Name |
| --- |
| ALF:HeraklezEval:Trojan:Win32/Lokibot |

| Name |
| --- |
| Emotet |

| Description |
| --- |
| [Emotet](https://attack.mitre.org/software/S0367) is a modular malware variant which is primarily used as a downloader for other malware variants such as [TrickBot](https://attack.mitre.org/software/S0266) and [IcedID](https://attack.mitre.org/software/S0483). Emotet first emerged in June 2014 and has been primarily used to target the banking sector. (Citation: Trend Micro Banking Malware Jan 2019) |

# Vulnerability

| Name |
| --- |
| CVE-2017-0199 |

| Name |
| --- |
| CVE-2017-11882 |

# Attack-Pattern

| Name |
| --- |
| Botnet |
| **ID** |
| T1583.005 |
| **Description** |
| Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing] (https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS). (Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter) |
| **Name** |
| TA0011 |
| **ID** |
| TA0011 |
| **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)

# External References

- https://otx.alienvault.com/pulse/64cc00feb8bd93677b5f4785
- https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/