



NETMANAGEIT

# Intelligence Report

# Shuckworm: Inside Russia's Relentless Cyber Campaign Against Ukraine



[T1566] Phishing



Ukraine



[T1059] Command and Scripting...



[T1547] Boot or Logon...



[T1091] Replication Through...



[T1105] Ingress Tool Transfer

# Table of contents

---

## Overview

---

● Description	3
● Confidence	3

---

---

## Entities

---

● Attack-Pattern	4
● Country	8

---

---

## External References

---

● External References	9
-----------------------	---

---

# Overview

## Description

The Shuckworm espionage group is continuing to mount multiple cyber attacks against Ukraine, with recent targets including security services, military, and government organizations. In some cases, Shuckworm has succeeded in staging long-running intrusions, lasting for as long as three months. The attackers repeatedly attempted to access and steal sensitive information such as reports about the deaths of Ukrainian military service members, enemy engagements and air strikes, arsenal inventories, military training, and more.

## 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**

Replication Through Removable Media

**ID**

T1091

**Description**

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself. Mobile devices may also be used to infect PCs with malware if connected via USB.(Citation: Exploiting Smartphone USB ) This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.(Citation: Windows Malware Infecting Android)(Citation: iPhone Charging Cable Hack) For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

**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**

Ingress Tool Transfer

**ID**

T1105

**Description**

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, `certutil`(https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `Invoke-WebRequest` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tfpt`, `rsync`, `finger`, and `wget`. (Citation: t1105\_lolbas)

**Name**

Command and Scripting Interpreter

**ID**

T1059

**Description**

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/techniques/T1059/004>) while Windows installations include the [Windows Command Shell](<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python](<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

# Country

**Name**

Ukraine



# External References

- 
- <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military>
- 
- <https://otx.alienvault.com/pulse/648b7609b129f88a8c939cc5>