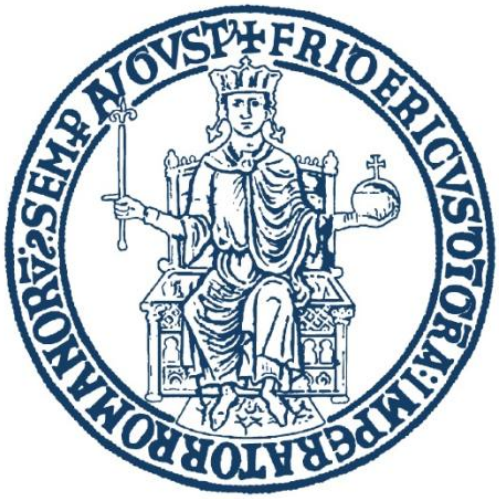

UNIVERSITÀ DEGLI STUDI
DI NAPOLI FEDERICO II

Università degli Studi di Napoli Federico II

Progetto di Software Security

Anno Accademico 2024/2025

Professori:

Prof. Roberto Natella

Studenti:

Riziero Graziani (M63001596)
Stefano Angelo Riviello (M63001592)
Andrea Esposito (M63001650)

Contents

1 Introduzione Analisi delle Minacce APT

Le **organizzazioni** sono sempre più frequentemente **bersaglio di attacchi avanzati e persistenti** (**APT**), che si caratterizzano per l'impiego di **strategie sofisticate**, suddivise in più fasi e supportate da **tecniche eterogenee**. Le fonti di **Cyber Threat Intelligence (CTI)**, come i **report sugli attacchi** e gli **articoli specializzati in cybersecurity**, offrono **informazioni importanti**. **Il presente lavoro** si propone di analizzare documenti di **threat intelligence** focalizzati su campagne di attacco condotte da gruppi **APT (Advanced Persistent Threat)**, al fine di identificare e comprendere l'uso delle vulnerabilità software sfruttate durante le varie fasi dell'attacco. **L'obiettivo finale** è presentare i risultati sotto forma di presentazione, evidenziando **pattern, tecniche e strumenti** comunemente usati nei cyberattacchi avanzati.

Per ogni **APT analizzato** verranno esaminati i seguenti aspetti:

1.1 Vulnerabilità sfruttate

- **CVE (Common Vulnerabilities and Exposures)**: identificatore univoco delle vulnerabilità.
- **CVSS (Common Vulnerability Scoring System)**: punteggio di gravità della vulnerabilità da 0 a 10.
- **CWE (Common Weakness Enumeration)**: categorizzazione delle debolezze software che causano vulnerabilità.
- **CPE (Common Platform Enumeration)**: identificazione univoca dei prodotti software/hardware vulnerabili.
- **EPSS (Exploit Prediction Scoring System)**: probabilità che una vulnerabilità venga sfruttata attivamente.
- **KEV (Known Exploited Vulnerabilities)**: elenco ufficiale delle vulnerabilità note come attivamente sfruttate.

Abbiamo sfruttato il progetto **CVSS-BT** per poter effettuare un'**analisi globale** delle **CVE** ed ottenere delle **metriche di vulnerabilità** più precise. Il progetto in questione

rilascia ogni giorno un nuovo file **CSV** con tutte le **metriche CVE aggiornate**. Per agevolare il nostro lavoro abbiamo realizzato uno **script Python** per consultare rapidamente tutte le informazioni disponibili su una specifica CVE.Di seguito riportiamo una **breve descrizione**:

- **Introduzione:**

  La gestione delle **vulnerabilità** non si basa solo sul punteggio **CVSS standard**, ma deve considerare anche informazioni aggiuntive come la **probabilità di exploit**, la **presenza di exploit pubblici** e l'effettivo sfruttamento *in-the-wild*. Il progetto **cvss-bt** arricchisce i dati CVSS integrando queste informazioni in un unico file **CSV** aggiornato periodicamente. Per maggiori informazioni, si consiglia di fare riferimento alla documentazione/**README** del progetto stesso.

  Questo script permette di **inserire l'ID di una CVE** e ottenere immediatamente tutte le informazioni correlate presenti nel file `cvss-bt.csv`, così da poter valutare con più accuratezza il **rischio reale** e la **priorità di intervento**.

- **Come funziona:**

  - Inserisci il file `cvss-bt.csv` (scaricabile dal repository cvss-bt) nella stessa cartella dello script.
  - Avvia lo **script Python**.
  - Inserisci l'**ID della CVE** richiesta (es: `CVE-2024-24919`).
  - Otterrai una stampa a video di tutte le **informazioni arricchite** per quella vulnerabilità.

- **Maggiori dettagli su cvss-bt:**

  Il tool **cvss-bt** serve per aiutarti a capire quanto è davvero pericolosa una **vulnerabilità (CVE)**, non solo guardando il punteggio **CVSS "base"** che vedi sul **National Vulnerability Database (NVD)**, ma anche tenendo conto di quante informazioni di **"minaccia reale"** ci sono su quella vulnerabilità, ad esempio se esistono **exploit pubblici**, se è già stata sfruttata da attaccanti, o se esistono **strumenti automatici** per sfruttarla.

- **Spiegazione dei campi:**

Campo	Spiegazione
`cve`	L'identificativo univoco della vulnerabilità (es: `CVE-2024-24919`).
`cvss-bt_score`	Il punteggio "**enriched**" **CVSS Base+Threat (CVSS-BT)**, cioè il punteggio CVSS base arricchito con le informazioni sulla minaccia effettiva (exploit, KEV, ecc). Più alto = più rischiosa/prioritaria.
`cvss-bt_severity`	Il livello di **severità** associato al punteggio CVSS-BT (es: HIGH, CRITICAL, MEDIUM).
`cvss-bt_vector`	La stringa **vettoriale** che descrive la composizione dettagliata del punteggio CVSS-BT secondo lo standard CVSS (quali metriche hanno contribuito). Può contenere anche una parte **E (Exploitability)** non presente nel base.
`cvss_version`	**Versione** dello standard CVSS usato (es: 3.1, 4.0).
`base_score`	Il punteggio **CVSS "base"**, cioè calcolato senza arricchimenti. È quello che trovi nel **NVD**.
`base_severity`	Livello di **severità** associato al base score (HIGH, CRITICAL, ecc).
`base_vector`	**Vettore CVSS base**, secondo lo standard, usato per calcolare il base score.
`assigner`	L'**ente/organizzazione** che ha pubblicato la CVE.
`published_date`	**Data di pubblicazione ufficiale** della CVE.
`epss`	Valore di **EPSS (Exploit Prediction Scoring System)**: una probabilità da 0 a 1 che la vulnerabilità venga effettivamente sfruttata nel mondo reale. Più alto = più probabile venga sfruttata.
`cisa_kev`	`True`/`False`: la vulnerabilità è presente nella lista delle vulnerabilità sfruttate attivamente secondo il catalogo **CISA KEV (Known Exploited Vulnerabilities)**. Se True, è già stata usata in attacchi reali!
`vulncheck_kev`	`True`/`False`: simile al campo sopra, ma secondo la fonte **VulnCheck KEV**.
`exploitdb`	`True`/`False`: la vulnerabilità ha un **exploit pubblico (PoC)** su **ExploitDB**.
`metasploit`	`True`/`False`: è disponibile un modulo per questa vulnerabilità su **Metasploit**, quindi può essere facilmente sfruttata tramite framework automatici.
`nuclei`	`True`/`False`: esiste un **template per il tool Nuclei** (scanner automatico), utile per automatizzare la rilevazione.
`poc_github`	`True`/`False`: esiste un **exploit proof-of-concept pubblico su GitHub** per questa vulnerabilità.

Il punteggio CVSS base (quello che trovi di solito nei siti ufficiali) dà un'idea di

quanto una vulnerabilità potrebbe essere pericolosa, ma non ti dice:

- Se esiste già un **exploit automatico**
- Se la vulnerabilità è stata già sfruttata **"sul campo"**
- Se esistono **strumenti pubblici** e facili da usare per attaccarla

Più precisamente il progetto CVSS-BT:

- Prende ogni **CVE** del catalogo NVD
- Per ogni CVE, cerca se:
  - Esistono **exploit pubblici** (su GitHub, ExploitDB, Metasploit...)
  - È già stata usata in **attacchi reali** (fonti come CISA KEV, VulnCheck KEV)
  - Esiste **codice funzionante e facile da usare** (come moduli Metasploit)
  - Ha un **punteggio EPSS alto** (cioè la probabilità che venga sfruttata è alta)
- Usa queste informazioni per **arricchire il punteggio CVSS base**, aggiungendo una componente chiamata **Exploitability/Exploit Code Maturity (E)**.

Perché conviene usarlo? Puoi vedere a colpo d'occhio non solo quanto potrebbe essere grave una vulnerabilità, ma anche quanto è probabile che venga sfruttata davvero, e se è già nel mirino degli attaccanti.

1.2 Cronologia della vulnerabilità

Per stabilire se fosse uno **zero-day** (vulnerabilità sconosciuta al pubblico e non patchata al momento dell'attacco) oppure già nota, specificando:

- La data di divulgazione pubblica.
- L'eventuale disponibilità di patch.
- Gli aggiornamenti su analisi e mitigazioni nel tempo.

1.3 Tecniche MITRE ATT&CK

Un framework che mappa le azioni degli attaccanti, tra cui:

- **Lateral Movement**
- **Privilege Escalation**
- **Initial Access**
- **Execution**
- e molte altre, a seconda del contesto.

1.4 Strumenti e tool

Utilizzati dagli attaccanti, come:

- **RAT (Remote Access Trojan)**
- **Strumenti di escalation dei privilegi**
- **Exploit kit specifici**

1.5 Prodotti vulnerabili

Definiamo:

- Se si tratta di un sistema operativo, software o hardware.
- Versioni affette e distribuzione dell'impatto sulla famiglia di prodotti.

1.6 Altri elementi utili

IOC (Indicators of Compromise) che sono informazioni tecniche, come indirizzi **IP**, **hash**, **domini** o **URL**, utilizzate per identificare e rilevare attività informatiche malevole. Eventuali **simulazioni realizzabili in laboratorio** per mostrare l'attacco.

2 APT29

Introduzione

APT29, noto anche come **Cozy Bear**, **The Dukes**, **NOBELIUM** o **Midnight Blizzard**, è un gruppo di cyber-spionaggio attribuito all'intelligence estera russa (**SVR**). Attivo almeno dal **2008**, è considerato uno degli attori più sofisticati nel panorama mondiale della **cybersicurezza**. I suoi **obiettivi principali** includono **governi**, **ambasciate** e **istituzioni diplomatiche**, oltre a **partiti politici** (come il **DNC durante le elezioni USA del 2016**), **centri di ricerca** – in particolare in ambito medico, inclusi quelli coinvolti nello sviluppo dei **vaccini COVID-19** – e **aziende tecnologiche**, come dimostrato nel celebre attacco alla **supply chain di SolarWinds nel 2020**. Le **tecniche utilizzate** comprendono lo **spear phishing**, ovvero email mirate per il furto di credenziali, l'impiego di **malware personalizzati** (tra cui **MiniDuke**, **CozyDuke** e **SeaDuke**), e l'uso di **canali di controllo camuffati** tramite servizi legittimi come **Twitter**, **GitHub** e **servizi cloud**. Le sue **caratteristiche distintive** includono un'estrema **sofisticazione** e **adattabilità**, la **capacità di mantenere accesso prolungato** ai sistemi compromessi e una **continua evoluzione delle tattiche** impiegate per evitare il rilevamento.
Tra i vari report di APT29 abbiamo analizzato quello che ci dava più informazioni.

2.1 F-Secure_Dukes_Whitepaper

Il report è un'analisi dettagliata delle attività del gruppo di cyber-spionaggio noto come **APT29** o "**The Dukes**", attivo dal **2008** e ritenuto collegato alla **Federazione Russa**. Questo gruppo ha condotto campagne di **spionaggio informatico** principalmente contro **governi occidentali**, **think tank**, **enti governativi**, ma anche contro **stati dell'ex URSS**, **governi asiatici**, **africani** e **mediorientali**, e perfino soggetti coinvolti nel **traffico di droga** o in **movimenti estremisti**.
Il documento analizza le varie famiglie di **malware** sviluppate e utilizzate dal gruppo (come **MiniDuke**, **CosmicDuke**, **OnionDuke**, **CozyDuke**, **CloudDuke**, **SeaDuke**, **HammerDuke**, **PinchDuke**, **GeminiDuke**), evidenziando la capacità del gruppo di **adattare rapidamente** i propri strumenti in risposta alle scoperte della **comunità di**

sicurezza.

Il **modus operandi** del gruppo comprende sia campagne massicce di **spear-phishing** che attacchi molto mirati e "chirurgici". Spesso, dopo un'intrusione rapida e rumorosa per raccogliere quanti più dati possibile, se il **target** risulta interessante, il gruppo passa a tecniche più **stealth** per una **presenza persistente** e una **raccolta dati a lungo termine**.

Il report mette in risalto anche la capacità di **resilienza** e l'"**arroganza**" del gruppo, che spesso continua ad usare strumenti anche dopo che questi sono stati scoperti pubblicamente, modificandoli solo minimamente per **eludere i controlli**.

2.2 Analisi Vulnerabilità

Nel corso dell'analisi di questo report sono state identificate le seguenti **vulnerabilità**:

Campo	Valore
cve	CVE-2010-0232
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2010-01-21T19:30Z
epss	0.73257
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-264: Permissions, Privileges, and Access Controls
cpe	Microsoft Windows NT, 2000 (SP4), XP (SP2/SP3), Server 2003 (SP2), Vista (SP1/SP2), Server 2008 (SP2), 7 (x86)

La vulnerabilità **CVE-2010-0232** riguarda diversi sistemi operativi **Windows** (**NT**, **2000**, **XP**, **Vista**, **Server 2003** e **2008**) e permette a un attaccante locale di ottenere **privilegi elevati**. È classificata come **grave**, con un punteggio **CVSS** di **7.8**, ed è ben documentata da **Microsoft**. Sono disponibili **exploit pubblici** e moduli in **ExploitDB** e **Metasploit**, mentre il rischio di sfruttamento è considerato piuttosto **alto**. La vulnerabilità è riconosciuta nei principali **database di sicurezza** (come **CISA** e **VulnCheck**) e riguarda i controlli di **permessi** e **privilegi** nel sistema operativo.

Campo	Valore
cve	CVE-2013-0640
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	psirt@adobe.com
published_date	2013-02-14T01:55Z
epss	0.92564
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	False
nuclei	False
poc_github	False
cwe	CWE-787: Out-of-Bounds Write
cpe	Adobe Reader/Acrobat 9.x, 10.x, 11.x

La vulnerabilità **CVE-2013-0640** colpisce **Adobe Reader** e **Acrobat** (versioni **9.x**, **10.x** e **11.x**) e consente la **scrittura fuori dai limiti della memoria**, un tipo di attacco spesso sfruttato per eseguire **codice malevolo**. Ha un livello di gravità **alto** (**CVSS 7.8**) ed è riconosciuta nei principali **database di sicurezza**. Sono disponibili **exploit pubblici** su **ExploitDB** e il rischio di sfruttamento è **elevato**, anche se non risultano moduli **Metasploit** pubblici associati.

Campo	Valore
cve	CVE-2013-0641
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	psirt@adobe.com
published_date	2013-02-14T01:55Z
epss	0.89391
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	False
nuclei	False
poc_github	False
cwe	CWE-120: Buffer Copy without Checking Size of Input
cpe	Adobe Acrobat Reader 9.x (incluso 9.1.x e 9.2–9.5.3)

La vulnerabilità **CVE-2013-0641** riguarda **Adobe Acrobat Reader 9.x** (comprese alcune versioni specifiche) e permette la copia di **buffer** senza controllare la dimensione dell'**input**, facilitando possibili attacchi di tipo **buffer overflow**. Il rischio è considerato **alto** (**CVSS 7.8**), la vulnerabilità è riconosciuta nei principali **database di sicurezza** e sono disponibili **exploit pubblici**. Tuttavia, non risultano exploit disponibili su **Metasploit** o **PoC** su **GitHub**.

Campo	Valore
cve	CVE-2010-4398
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
assigner	cve@mitre.org
published_date	2010-12-06T13:44Z
epss	0.12282
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	False
nuclei	False
poc_github	False
cwe	CWE-787: Out-of-bounds Write
cpe	Microsoft Windows XP (SP2 Professional x64 e SP3), Windows Server 2003 (SP2), Windows Vista (SP1, SP2), Windows Server 2008 (tutte le versioni, incl. R2, SP2), Windows 7

La vulnerabilità **CVE-2010-4398** riguarda diversi sistemi operativi **Windows**, tra cui **XP**, **Server 2003**, **Vista**, **Server 2008** e **Windows 7**. Permette la **scrittura fuori dai limiti della memoria** (**out-of-bounds write**), con un rischio considerato **alto** (**CVSS 7.8**). È stata riconosciuta dai principali **database di sicurezza**, sono disponibili **exploit pubblici**, ma non risultano exploit su **Metasploit** né **proof-of-concept** su **GitHub**. Il rischio di sfruttamento è **medio-basso** rispetto ad altre vulnerabilità simili.

Le informazioni temporali relative a **F-Secure Dukes** sono le seguenti :

Punto	**Dettaglio**
Tipo	Vulnerabilità di escalation dei privilegi in Microsoft Windows tramite il driver `win32k.sys`.
Divulgazione	Divulgata pubblicamente a gennaio 2010. Disclosure e PoC pubblici di Tavis Ormandy il 19 gennaio 2010.
Zero day?	Non era zero day al momento dell'utilizzo noto da parte dei Dukes (CosmicDuke lo ha sfruttato dopo la pubblicazione pubblica).
Patch	Microsoft ha rilasciato una patch per CVE-2010-0232 tramite aggiornamento di sicurezza MS10-015 pubblicato il 9 febbraio 2010.
Utilizzo nel malware	Utilizzata da CosmicDuke nel 2010, almeno una settimana dopo la divulgazione pubblica e la pubblicazione del PoC. Quindi colpiva solo sistemi non aggiornati.

Table 1: Dettagli temporali per CVE-2010-0232

Punto	**Dettaglio**
Tipo	Vulnerabilità di tipo Out-of-bounds Write nel driver `win32k.sys` su sistemi Windows.
Divulgazione	Divulgata pubblicamente nel dicembre 2010. PoC pubblico già disponibile online poco dopo la disclosure.
Zero day?	Non era zero day al momento dell'utilizzo documentato nei Dukes; patch e PoC già pubblici.
Patch	Microsoft ha rilasciato la patch di sicurezza relativa nel 2011 tramite MS11-034.
Utilizzo nel malware	Sfruttata da CosmicDuke dopo la pubblicazione pubblica della vulnerabilità. Quindi targeting su sistemi privi di patch.

Table 2: Dettagli temporali per CVE-2010-4398

Punto	Dettaglio
Tipo	Vulnerabilità di esecuzione di codice remoto in Adobe Reader e Acrobat, sfruttabili tramite PDF malevoli.
Divulgazione	Divulgate pubblicamente il 12 febbraio 2013, con advisory Adobe e comunicati FireEye e Kaspersky.
Zero day?	Utilizzate come zero-day inizialmente: i primi attacchi documentati (tra cui quelli del gruppo Dukes/MiniDuke) precedono la pubblicazione della patch e dell'advisory.
Patch	Adobe ha pubblicato la patch il 20 febbraio 2013 (Security Bulletin APSB13-07).
Utilizzo nel malware	Utilizzate attivamente in campagne spear-phishing di MiniDuke tra il 12 e il 20 febbraio 2013, sia prima che dopo la disclosure pubblica.

Table 3: Dettagli temporali per CVE-2013-0640 e CVE-2013-0641

2.3 TTP MITRE ATT&CK

Le TTP che abbiamo rilevato sono le seguenti :

ID	Tactic	Technique	Sub-technique	Descrizione
001	INITIAL ACCESS (TA0001)	PHISHING (T1566)	ATTACHMENT (T1566.001)	Utilizzo di documenti Microsoft Word e PDF appositamente creati come allegati email malevoli per infiltrare organizzazioni target.
002	EXECUTION (TA0002)	SYSTEM SERVICES (T1569)	SERVICE EXECUTION (T1569.002)	Creazione e scrittura di un eseguibile malevolo su disco e successiva esecuzione.

003	DISCOVERY (TA0007)	SYSTEM INFORMATION DISCOVERY (T1082)	—	Raccolta di informazioni sul sistema compromesso.
004	EXFILTRATION (TA0010)	EXFILTRATION OVER C2 CHANNEL (T1041)	—	Esfiltrazione di dati attraverso un canale di comando e controllo (C&C).
004	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	—	Esecuzione di comandi remoti sulla macchina compromessa.
005	INITIAL ACCESS (TA0001)	PHISHING (T1566)	ATTACHMENT (T1566.001)	Uso di allegati di spearphishing per consegnare malware.
006	CREDENTIAL ACCESS (TA0006)	CREDENTIAL DUMPING (T1003)	—	Raccolta di credenziali tramite varie tecniche.
007	IMPACT (TA0040)	ENDPOINT DENIAL OF SERVICE (T1499)	—	Utilizzo di attacchi DoS per compromettere o limitare la disponibilità dei sistemi.
008	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Uso di link in email di spearphishing per indurre le vittime a visitare siti compromessi o scaricare malware.
009	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Utilizzo di una email di spearphishing contenente un link a un archivio zip ospitato su cloud (DropBox).

010	RESOURCE DEVELOPMENT (TA0042)	COMPROMISE INFRASTRUCTURE (T1584)	—	Il nodo Tor compromesso modifica eseguibili scaricati tramite connessioni HTTP per introdurre malware.
011	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	WEB PROTOCOLS (T1071.001)	Uso di connessioni HTTP per scaricare eseguibili.
012	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	Gli eseguibili modificati vengono eseguiti dalle vittime, risultando nell'infezione.
013	DISCOVERY (TA0007)	SYSTEM OWNER/USER DISCOVERY (T1033)	—	Capacità di OnionDuke di raccogliere informazioni sul sistema e di tentare di rubare username e password delle vittime.
013	IMPACT (TA0040)	NETWORK DENIAL OF SERVICE (T1498)	—	Uno dei moduli di OnionDuke è progettato per eseguire attacchi DoS.
014	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Invio di email di spear-phishing contenenti link malevoli che portano a un sito compromesso che ospita CozyDuke.
017	COMMAND AND CONTROL (TA0011)	WEB SERVICE (T1102)	—	Comunicazione con server C&C tramite HTTP o HTTPS per scaricare comandi da eseguire (HammerDuke, variante semplice).

019	LATERAL MOVEMENT (TA0008)	REMOTE SERVICES (T1021)	—	Uso di servizi remoti per eseguire comandi su macchine compromesse (CloudDuke).
021	COLLECTION (TA0009)	DATA FROM LOCAL SYSTEM (T1005)	—	Attività di raccolta dati da un sistema locale (PinchDuke).
022	EXFILTRATION (TA0010)	EXFILTRATION OVER COMMAND AND CONTROL CHANNEL (T1041)	—	Uso di canali di comando e controllo per esfiltrare dati rubati dal sistema compromesso.
023	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	WEB PROTOCOLS (T1071.001)	Uso di protocolli web (HTTP/HTTPS) per comunicazioni C&C e trasferimento dati esfiltrati.
024	COLLECTION (TA0009)	DATA FROM LOCAL SYSTEM (T1005)	—	Raccolta di dati dal sistema locale, come file creati in un dato periodo con estensioni specifiche.
026	DISCOVERY (TA0007)	SYSTEM INFORMATION DISCOVERY (T1082)	—	Raccolta di informazioni di sistema sulla configurazione del computer della vittima (GeminiDuke).
028	COLLECTION (TA0009)	INPUT CAPTURE (T1056)	—	Keylogging, ovvero la cattura dei dati di input utente.
029	COLLECTION (TA0009)	SCREEN CAPTURE (T1113)	—	Cattura di screenshot del desktop o di finestre specifiche.
030	COLLECTION (TA0009)	CLIPBOARD DATA (T1115)	—	Furto del contenuto della clipboard di sistema.

031	COLLECTION (TA0009)	DATA FROM LOCAL SYSTEM (T1005)	—	Raccolta di dati dal sistema locale, inclusi file utente con estensioni specifiche.
032	CREDENTIAL ACCESS (TA0006)	CREDENTIALS FROM PASSWORD STORES (T1555)	CREDENTIALS FROM WEB BROWSERS (T1555.003)	Furto delle credenziali salvate nei browser web.
033	EXFILTRATION (TA0010)	EXFILTRATION OVER ALTERNATIVE PROTOCOL (T1048)	—	Uso di protocolli alternativi per esfiltrare dati rubati (HTTP, HTTPS, FTP o WebDav).
034	EXFILTRATION (TA0010)	EXFILTRATION OVER COMMAND AND CONTROL CHANNEL (T1041)	—	Uso di un canale C&C per esfiltrare i dati raccolti verso un server remoto.

2.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti.Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
MINIDUKE	S0051	Trojan modulare APT, utilizzato come loader di terzo stadio nelle campagne CosmiDuke, noto per impieghi in attacchi mirati contro istituzioni governative europee; permette esecuzione di comandi remoti sul sistema compromesso.
COSMICDUKE	S0050	Malware che combina codice della famiglia MiniDuke (loader) e componenti info-stealer, utilizzato per furto di credenziali, dati locali, keylogging, screenshot, e persistenza tramite diversi vettori di attacco. Permette anche privilege escalation, esfiltrazione via diversi protocolli (HTTP, HTTPS, FTP, WebDav).
ONIONDUKE	S0052	Tool modulare con funzionalità di furto credenziali, attacchi DoS, raccolta informazioni, dropper e diffusione tramite torrent o Tor node compromessi; permette credential dumping e attacchi di impatto (DoS).
COZYDUKE	S0046	Malware modulare che utilizza moduli scaricabili da C&C per dotarsi delle funzionalità necessarie; impiegato in spear-phishing con link malevoli e raccolta iniziale di informazioni.
CLOUDDUKE	S0054	Toolset composto da loader, downloader e backdoor, consente l'esecuzione remota di comandi, anche tramite OneDrive per la comunicazione C&C, rendendo difficile il blocco del traffico malevolo.

Tool	ID MITRE	Descrizione
SEADUKE	S0053	Backdoor multipiattaforma scritta in Python, utilizzabile sia su sistemi Windows che Linux, impiegata per accesso persistente e controllo remoto.
HAMMERDUKE	S0037	Backdoor Windows-only (scritta in .NET), in grado di comunicare tramite HTTP/S o Twitter per recuperare comandi da eseguire; pensata per persistenza e controllo delle vittime.
PINCHDUKE	S0048	Toolset che include loader e trojan infostealer, raccoglie configurazioni di sistema, file, credenziali, e le esfiltra via HTTP/S; utilizzato nelle campagne iniziali (dal 2008) soprattutto per furto credenziali e raccolta dati locali.
GEMINIDUKE	S0049	Info-stealer focalizzato sulla raccolta di informazioni di sistema, utenti, configurazioni di rete, processi e file; include componenti di persistenza personalizzati.

Table 5: Tool associati al gruppo Dukes

2.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
Microsoft Windows	Sistema Operativo	Vulnerabilità di esecuzione di codice tramite file malevoli (doc, pdf, eseguibili, ecc.), inclusi exploit di privilege escalation (es. CVE-2010-0232, CVE-2010-4398) e social engineering (phishing via documenti Office, PDF, ecc).
Adobe Reader	Applicazione	Vulnerabilità di esecuzione di codice tramite PDF malevoli, spesso sfruttando vulnerabilità 0-day (es. CVE-2013-0640, CVE-2013-0641).
Adobe Acrobat	Applicazione	Vulnerabilità di esecuzione di codice tramite file PDF modificati.

Table 6: Prodotti vulnerabili e principali note sulle vulnerabilità sfruttate dalle campagne Dukes

2.6 IoC

Gli *Indicators of Compromise* (IoC) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del report originale, all'interno dell'appendice. In questa sezione finale del PDF è possibile trovare esempi di hash, nomi di file, URL malevoli, domini di command and control, percorsi di debug e altri indicatori tecnici associati alle varie famiglie di malware descritte nel rapporto.

2.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, 'e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell'attacco:

Fase	Tool suggerito	Note operative
Simulazione spear-phishing	GoPhish	Invio di email di phishing con allegati o link malevoli, monitoraggio delle aperture e dei click.
Generazione documenti/attachment malevoli	Metasploit	Creazione di file Word/PDF con macro o exploit, payload per l'accesso remoto.
Privilege escalation	Metasploit (exploit)	Esecuzione di exploit locali (es. CVE-2010-0232) per ottenere privilegi amministrativi.
Credential dumping	Mimikatz	Estrazione di password e hash da memoria e programmi installati.
Keylogging e raccolta dati utente	PyKeylogger	Registrazione dei tasti premuti, screenshot, raccolta dati dalla clipboard.
Persistenza	Metasploit persistence	Installazione di backdoor o persistence fileless per il mantenimento dell'accesso.
Command and Control (C2)	Metasploit	Gestione delle sessioni di controllo remoto, invio di comandi, ricezione dati.
Esfiltrazione dati	Metasploit	Esportazione di file e informazioni sensibili tramite cloud, HTTP/S o DNS.
Simulazione botnet/DoS	Hping3, Metasploit auxiliary	Test di attacchi DoS a scopo di laboratorio su target controllati.

Table 7: Tool consigliati per la simulazione in ambiente di laboratorio

3 APT Carbanak

Introduzione

Carbanak è uno dei gruppi di **cybercriminali** più famosi e temuti degli ultimi anni. Attivo dal 2013 circa, questo gruppo ha preso di mira soprattutto **banche e istituzioni finanziarie** in tutto il mondo, riuscendo a rubare cifre che superano complessivamente il **miliardo di dollari**. Il loro metodo principale era l'invio di **email trappola (phish-**

ing) a dipendenti delle banche: bastava che una sola persona aprisse il file allegato per permettere agli hacker di infiltrarsi nella rete interna della banca.Una volta dentro, Carbanak **studiava i sistemi** per settimane o mesi, controllando in modo quasi invisibile le attività degli operatori. Poi agiva con grande precisione, riuscendo a **prelevare soldi direttamente dai bancomat**, a **effettuare bonifici** verso conti controllati dal gruppo, o a **manipolare i dati** per coprire i furti.Dopo anni di attività e vari adattamenti delle loro tecniche, nel 2018 è stato arrestato quello che si ritiene fosse il **capo dell'organizzazione**. L'operazione Carbanak ha lasciato il segno nella storia della **sicurezza informatica**, diventando un **caso di studio** su come anche le banche più sicure possano essere vulnerabili di fronte ad attacchi così sofisticati.

3.1 Carbanak_APT

Il report analizza una vasta campagna di cyberattacchi, iniziata dal 2013, che ha colpito **banche e istituzioni finanziarie in tutto il mondo**, generando perdite fino a **un miliardo di dollari**. Gli attacchi sono stati realizzati da **un gruppo criminale sconosciuto** con motivazione principalmente finanziaria, utilizzando **tecniche avanzate tipiche delle APT** (Advanced Persistent Threats).

La compromissione iniziava tramite **email di spear phishing** con allegati malevoli, che sfruttavano vulnerabilità di **Microsoft Office** per eseguire codice dannoso. Una volta infettato il sistema, veniva installato il malware **Carbanak**, utilizzato per ottenere accesso remoto, esfiltrare dati e controllare i computer delle vittime.

Successivamente, gli attaccanti si muovevano lateralmente nella rete, acquisendo credenziali e sfruttando strumenti come **Ammyy Admin**, **Mimikatz**, **Metasploit** e **PsExec** per raggiungere i sistemi critici (ATM, SWIFT, database).

L'obiettivo finale era **monetizzare l'accesso**: i criminali eseguivano bonifici fraudolenti, manipolavano database o comandavano agli **ATM di dispensare contanti** a complici. Dal punto di vista tecnico, **Carbanak** si mascherava come processi di sistema, cancellava le tracce, acquisiva video e screenshot delle attività degli operatori bancari e comunicava in modo cifrato con i server di comando e controllo.

Il malware restava attivo per mesi, permettendo azioni mirate e difficili da rilevare. **Oltre 100 banche sono state colpite**, con perdite per singolo istituto fino a milioni di dollari. Gli attaccanti limitavano i prelievi a **massimo 10 milioni di dollari per vittima** per

ridurre il rischio di indagini approfondite.

3.2 Analisi Vulnerabilita‘

Nel corso dell'analisi di questo report sono state identificate le seguenti vulnerabilita':

Campo	Valore
cve	CVE-2012-0158
cvss-bt_score	8.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	8.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2012-04-10T21:55Z
epss	0.94295
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-94: Improper Control of Generation of Code ('Code Injection')
cpe	Microsoft Office (Word, Excel, altri componenti) fino a Office 2010

La vulnerabilità **CVE-2012-0158** interessa **Microsoft Office** (**Word**, **Excel** e altri componenti) fino alla versione **2010**. È molto **grave** (**CVSS 8.8**) e permette l'**iniezione di codice**, potenzialmente consentendo l'**esecuzione di comandi arbitrari** sul sistema. Il rischio di sfruttamento è **elevato**, con **exploit** e **PoC** pubblici disponibili e presenza nei principali **database di sicurezza**. È ampiamente riconosciuta come una delle vulnerabilità più **sfruttate** su **Office**.

Campo	Valore
cve	CVE-2013-3906
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2013-11-06T15:55Z
epss	0.92857
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	False
cwe	CWE-94:Improper Control of Generation of Code ('Code Injection')
cpe	Microsoft Office 2007 SP3, 2010 SP1/SP2, 2013; Windows Server 2008/2012; Lync 2010/2013; altri prodotti Microsoft Office e Windows

La vulnerabilità **CVE-2013-3906** colpisce vari prodotti **Microsoft**, tra cui **Office 2007/2010/2013**, **Windows Server 2008/2012** e **Lync**. Consente l'**iniezione di codice** (**code injection**) con un rischio **alto** (**CVSS 7.8**). È ampiamente riconosciuta nei principali **database di sicurezza** e sono disponibili **exploit pubblici**, anche se non risultano **PoC** su **GitHub**. Il rischio di sfruttamento è **elevato** e riguarda sia **Office** che **Windows**.

Campo	Valore
cve	CVE-2014-1761
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2014-03-25T13:24Z
epss	0.92944
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	False
cwe	CWE-787: Out-of-bounds Write
cpe	Microsoft Word 2003, 2007, 2010, 2013; Word Viewer; Office per Mac 2011; Office Web Apps; SharePoint Server

La vulnerabilità **CVE-2014-1761** interessa diversi prodotti **Microsoft**, tra cui **Word** (**2003**, **2007**, **2010**, **2013**), **Word Viewer**, **Office per Mac 2011**, **Office Web Apps** e **SharePoint Server**. È di tipo "**out-of-bounds write**" e può consentire l'**esecuzione di codice dannoso**. Il rischio è **alto** (**CVSS 7.8**), sono disponibili **exploit pubblici** e moduli **Metasploit**, ed è ampiamente riconosciuta nei **database di sicurezza**.

Campo	Valore
cve	CVE-2013-3660
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	cve@mitre.org
published_date	2013-05-24T20:55Z
epss	0.67944
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-119: Improper Restriction of Operationsthe Bounds of a Memory Buffer
cpe	Windows XP SP2/SP3, Vista SP2, 7 SP1, 8, Server 2003 SP2, Server 2008 SP2/R2 SP1, Server 2012.

La vulnerabilità **CVE-2013-3660** riguarda vari sistemi **Windows** (**XP**, **Vista**, **7**, **Server 2003/2008/2012**) e deriva da una gestione non corretta della **memoria**, che può portare all'**esecuzione di codice malevolo**. Ha un rischio **alto** (**CVSS 7.8**), è riconosciuta dai principali **database di sicurezza**, ma al momento non risultano **exploit pubblici** né moduli **Metasploit** o **PoC** su **GitHub**.

Le informazioni temporali relative CVE di **Carbanak APT** sono le seguenti:

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice in Microsoft Office (Word, Excel, ecc.), sfruttata tramite allegati .doc malevoli in spear phishing.
Divulgazione	Divulgata pubblicamente ad aprile 2012.
Zero day?	Non era zero day al momento degli attacchi Carbanak: la vulnerabilità era nota e con patch disponibile già da tempo.
Patch	Microsoft ha rilasciato la patch MS12-027 il 10 aprile 2012 per correggere la vulnerabilità.
Utilizzo nel malware	Sfruttata nei primi attacchi Carbanak tramite allegati .doc malevoli, targeting utenti di istituzioni finanziarie che non avevano applicato la patch.

Table 8: Informazioni temporali per CVE-2012-0158

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice in Microsoft Office tramite file .doc e .cpl.
Divulgazione	Divulgata pubblicamente a novembre 2013.
Zero day?	Non era zero day per Carbanak: la vulnerabilità era già pubblica e patchata al momento degli attacchi.
Patch	Microsoft ha rilasciato la patch MS13-096 il 12 novembre 2013.
Utilizzo nel malware	Sfruttata tramite spear phishing in allegati Office per installare il malware Carbanak su sistemi non aggiornati.

Table 9: Informazioni temporali per CVE-2013-3906

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice remoto in Microsoft Word.
Divulgazione	Divulgata pubblicamente ad aprile 2014.
Zero day?	Non era zero day per Carbanak: la vulnerabilità era nota e con patch disponibile.
Patch	Microsoft ha rilasciato la patch MS14-017 l'8 aprile 2014.
Utilizzo nel malware	Utilizzata per compromettere le vittime tramite spear phishing, targeting sistemi privi di patch.

Table 10: Informazioni temporali per CVE-2014-1761

Punto	**Dettaglio**
Tipo	Vulnerabilità di privilege escalation su Windows (Win32k.sys).
Divulgazione	Divulgata pubblicamente a giugno 2013.
Zero day?	Non era zero day al momento degli attacchi Carbanak: la vulnerabilità era pubblica e con patch.
Patch	Microsoft ha pubblicato la patch MS13-053 l'11 giugno 2013.
Utilizzo nel malware	Utilizzata da Carbanak per ottenere privilegi amministrativi dopo l'infezione iniziale, su sistemi non aggiornati.

Table 11: Informazioni temporali per CVE-2013-3660

3.3 TTP MITRE ATTCK

Le TTP che abbiamo rilevato sono le seguenti :

ID	**Tactic**	**Technique**	**Sub-technique**	**Descrizione**
001	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di email di phishing con allegati malevoli per compromettere il sistema della vittima.

002	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	—	Sfruttamento di vulnerabilità su software client (es. lettore documenti) per eseguire codice arbitrario.
003	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	—	Utilizzo di interpreti di comandi/script per eseguire comandi e script malevoli.
005	LATERAL MOVEMENT (TA0008)	REMOTE SERVICES (T1021)	—	Gli attaccanti usano servizi remoti per spostarsi lateralmente nella rete compromessa.
039	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	Il shellcode esegue il backdoor Carbanak.
006	COLLECTION (TA0009)	VIDEO CAPTURE (T1125)	—	Gli attaccanti acquisiscono video dal sistema della vittima, spesso per sorveglianza o raccolta credenziali/informazioni sensibili.
007	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	—	Comunicazione con il server di comando e controllo (C2).
040	DEFENSE EVASION (TA0005), PRIVILEGE ESCALATION (TA0004)	ACCESS TOKEN MANIPULATION (T1134)	TOKEN IMPERSONATION/THEFT (T1134.001)	Gli attaccanti abusano dei servizi impersonando utenti locali legittimi per eseguire azioni privilegiate.

008	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di email di phishing con allegati malevoli per compromettere il sistema della vittima.
009	COMMAND AND CONTROL (TA0011)	INGRESS TOOL TRANSFER (T1105)	—	Trasferimento di strumenti/file dall'esterno al sistema compromesso.
010	COLLECTION (TA0009)	VIDEO CAPTURE (T1125)	—	Carbanak utilizza componenti di spionaggio per controllare la webcam/video del sistema vittima.
011	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di email di phishing con allegati malevoli per compromettere il sistema della vittima.
012	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	—	Sfruttamento di vulnerabilità software per eseguire codice sul sistema della vittima.
013	INITIAL ACCESS (TA0001), DEFENSE EVASION (TA0005)	VALID ACCOUNTS (T1078)	—	Utilizzo di account validi per ottenere accesso non autorizzato ai sistemi.
014	COMMAND AND CONTROL (TA0011)	INGRESS TOOL TRANSFER (T1105)	—	Trasferimento di strumenti/file da sistemi esterni a sistemi interni nella rete vittima.
016	DEFENSE EVASION (TA0005)	MASQUERADING (T1036)	MATCH LEGITIMATE NAME OR LOCATION (T1036.005)	L'attaccante rinomina file malevoli con nomi legittimi per eludere il rilevamento.

017	DEFENSE EVASION (TA0005)	HIDE ARTIFACTS (T1564)	HIDDEN FILES AND DIRECTORIES (T1564.001)	L'attaccante nasconde file e directory per renderli invisibili a utenti e strumenti di sicurezza.
018	DEFENSE EVASION (TA0005)	INDICATOR REMOVAL ON HOST (T1070)	FILE DELETION (T1070.004)	L'attaccante elimina file per cancellare le tracce e ostacolare le indagini.
019	—	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Creazione o modifica di un servizio per ottenere persistenza ed esecuzione automatica.
020	DEFENSE EVASION (TA0005)	MASQUERADING (T1036)	—	Cambio nome di file/processi per farli apparire legittimi.
021	DISCOVERY (TA0007)	PROCESS DISCOVERY (T1057)	—	Carbanak identifica processi specifici associati a software di sicurezza (es. Kaspersky).
022	PERSISTENCE (TA0003), PRIVILEGE ESCALATION (TA0004)	REGISTRY RUN KEYS / STARTUP FOLDER (T1060)	—	Uso di chiavi di registro per esecuzione comandi o caricamento automatico all'avvio.
023	PRIVILEGE ESCALATION (TA0004), DEFENSE EVASION (TA0005)	PROCESS INJECTION (T1055)	—	Carbanak inietta codice nel processo svchost.exe per mascherare le sue attività.

024	EXFILTRATION (TA0010)	EXFILTRATION OVER C2 CHANNEL (T1041)	—	Carbanak comunica con il suo C2 per scaricare file di configurazione da monitorare.
025	COLLECTION (TA0009)	INPUT CAPTURE (T1056)	—	Carbanak registra i tasti digitati per raccogliere credenziali e informazioni sensibili.
026	COLLECTION (TA0009)	SCREEN CAPTURE (T1113)	—	Carbanak cattura screenshot del desktop ogni 20 secondi.
027	EXECUTION (TA0002)	SYSTEM SERVICES (T1569)	—	Carbanak imposta il servizio Termservice in modalità avvio automatico.
028	—	PROCESS INJECTION (T1055)	—	Modifica codice eseguibile in memoria per processi locali/remoti simultanei.
029	DISCOVERY (TA0007)	PROCESS DISCOVERY (T1057)	—	Carbanak rileva la presenza dell'applicazione bancaria BLIZKO.
030	IMPACT (TA0040)	DATA MANIPULATION (T1565)	STORED DATA MANIPULATION (T1565.001)	Carbanak può manipolare i dettagli dei documenti di pagamento nel sistema IFOBS.
031	EXFILTRATION (TA0010)	EXFILTRATION OVER C2 CHANNEL (T1041)	—	Carbanak usa HTTP per comunicare con il C2 e inviare dati raccolti.
032	COMMAND AND CONTROL (TA0011)	DATA ENCODING (T1132)	—	Carbanak usa cifratura RC2+Base64 per cifrare i dati trasmessi nel canale C2.

033	COMMAND AND CONTROL (TA0011)	REMOTE ACCESS TOOL (T1219)	—	Uso di Ammyy Admin come tool di amministrazione remota per controllare i sistemi nella rete compromessa.
034	LATERAL MOVEMENT (TA0008)	REMOTE ACCESS TOOL (T1021)	SSH (T1021.004)	Uso di SSH per accessi remoti non autorizzati a sistemi compromessi.
038	COLLECTION (TA0009)	VIDEO CAPTURE (T1125)	—	Cattura video delle azioni dell'utente su un sistema infetto.

3.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti.Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
CARBANAK	S0030	Backdoor modulare usata per accesso remoto, esecuzione comandi, raccolta dati, video/screen/keylogger, manipolazione servizi, persistence e data exfiltration.
AMMYY	—	Tool legittimo di remote administration (Ammyy Admin), usato dagli attaccanti per controllo remoto della rete compromessa, sfruttando la sua diffusione nei contesti enterprise.
METASPLOIT	—	Framework di penetration testing, usato per movimenti laterali, sfruttamento di vulnerabilità, escalation di privilegi e upload di payload personalizzati nella rete delle vittime.

Continua nella pagina successiva

Tool	ID MITRE	Descrizione
PSEXEC	S0029	Tool di amministrazione remota Microsoft, sfruttato per esecuzione comandi/processi da remoto e movimenti laterali attraverso la rete.
MIMIKATZ	S0002	Strumento usato per il dump e furto di credenziali da memoria su sistemi Windows compromessi.
SSH (backdoor)	—	SSH ricompilato/backdoorizzato per accesso remoto persistente su host Linux/Unix nella rete vittima.

Table 13: Tool utilizzati

3.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
Microsoft Windows	Sistema Operativo	Vulnerabilità di esecuzione di codice tramite file malevoli (doc, pdf, cpl, ecc.), inclusi exploit di privilege escalation (es. CVE-2013-3660) e tecniche di social engineering (phishing via documenti Office, PDF, ecc.). Utilizzati anche servizi remoti (RDP, SSH) per movimenti laterali.
Microsoft Office (Word 2003, 2007, 2010)	Applicazione	Vulnerabilità di esecuzione di codice tramite exploit su allegati malevoli (es. CVE-2012-0158, CVE-2013-3906, CVE-2014-1761), sfruttate per ottenere l'accesso iniziale tramite spear phishing.
Oracle Database	Database	Manipolazione dei database per l'apertura di conti fittizi, trasferimento fondi e alterazione dati senza sfruttare bug software ma abusando di accessi compromessi.
ATM (Automated Teller Machine) Network	Infrastruttura Finanziaria	Accesso remoto abusivo tramite sistemi Windows compromessi collegati in VPN alla rete ATM; esecuzione di operazioni non autorizzate (cash out) senza installare malware sugli ATM stessi.

Table 14: Prodotti vulnerabili nelle campagne Carbanak

3.6 IoC

Gli **Indicators of Compromise** (**IoC**) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del **report originale**, all'interno dell'**appendice**. In questa sezione finale del **PDF**(pagine 27-37) è possibile trovare esempi di **hash**, **nomi di file**, **URL** malevoli, **domini** di **command and control**, **percorsi di debug** e altri indicatori tecnici associati alle varie famiglie di **malware** descritte nel rapporto.

3.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, ‘e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell’attacco:

Fase	**Tool suggerito**	**Note operative**
Simulazione spear-phishing	GoPhish, SET	Invio di email di phishing con allegati Word/CPL malevoli exploitabili (es. CVE-2012-0158, CVE-2013-3906, CVE-2014-1761), raccolta dati su click e aperture.
Generazione documenti/attachment malevoli	Metasploit, MS Office, Luckystrike	Creazione di file Word/PDF con macro o exploit, payload custom per accesso remoto, generazione automatica di CPL malevoli.
Esecuzione del payload	Metasploit, Carbanak Loader	Sfruttamento delle vulnerabilità client per ottenere esecuzione codice remoto sul sistema vittima e installazione della backdoor Carbanak.
Movimento laterale	PsExec, Metasploit, Ammyy Admin, SSH	Utilizzo di tool per esecuzione remota comandi, movimenti laterali, deploy di payload su host interni (Windows e Linux). Possibile abuso di credenziali raccolte.
Raccolta dati	Carbanak, Mimikatz, Ammyy Admin	Keylogger, video e screen capture, raccolta credenziali e file sensibili; uso di Ammyy Admin per accesso interattivo remoto.
Persistence	Carbanak, registry tools, servizi Windows	Creazione di servizi/chiavi di registro per persistenza; iniezione in processi legittimi (es. svchost.exe) per evadere detection.

Continua nella pagina successiva

Fase	Tool suggerito	Note operative
Command and Control	Carbanak, Ammyy Admin, SSH backdoor	Comunicazioni con C2 tramite HTTP(s) con dati cifrati RC2+Base64; amministrazione remota tramite Ammyy/SSH.
Exfiltration	Carbanak, Ammyy Admin, RDP	Esfiltrazione dati via HTTP(s), download-/upload file via Ammyy Admin, uso di tunnel RDP per l'estrazione massiva.
Impatto finale (manipolazione dati/frode)	Carbanak, tool SQL/DB, tool bancari interni	Manipolazione database (es. Oracle, IFOBS), creazione di transazioni fraudolente o cashout ATM.

Table 15: Fasi, tool suggeriti e note operative per simulare una campagna Carbanak

4 APT Oilrig

Introduzione

OilRig (noto anche come **APT34** o **Helix Kitten**) è un gruppo di cyber-spionaggio legato all'Iran, attivo dal 2014 e conosciuto per attacchi mirati soprattutto in Medio Oriente. Il gruppo prende di mira settori strategici come **enti governativi, energia, finanza e telecomunicazioni**, focalizzandosi sui Paesi del Golfo, ma con attacchi anche verso Europa e Nord America. OilRig si distingue per la capacità di **adattare e aggiornare rapidamente** le proprie tecniche di attacco, utilizzando principalmente **campagne di spear phishing**, cioè email mirate per rubare credenziali o installare malware. Tra i malware più usati ci sono backdoor personalizzate come **Helminth, QUADAGENT e STEALHOOK**, che permettono agli attaccanti di mantenere un **accesso prolungato e nascosto** alle reti compromesse. Dopo l'accesso iniziale, il gruppo si muove lateralmente nella rete usando **tecniche di escalation dei privilegi** e strumenti come **Mimikatz** per compromettere altre credenziali e ottenere il controllo su una porzione più ampia della rete. L'obiettivo principale di OilRig è l'**esfiltrazione di dati sensibili**, spesso tramite canali nascosti come il **tunneling DNS**, a supporto degli interessi geopolitici iraniani. Negli ultimi anni, OilRig ha dimostrato un'elevata **sofisticazione**, sfruttando rapidamente nuove vulnerabilità. Rimane una delle minacce più

rilevanti per le **organizzazioni che operano in settori critici**, richiedendo attenzione e difese sempre aggiornate.

4.1 APT34 The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations

Il report analizza le attività del gruppo **APT34**, un gruppo di **cybercriminali** attivo dal **2014** e attribuito all'**Iran**. Il gruppo è noto per aver preso di mira soprattutto organizzazioni e **infrastrutture critiche** in **Medio Oriente** (ma non solo), tra cui settori come **tecnologia**, **governo**, **militare**, **energia**, **comunicazioni**, **trasporti**, **finanza** ed **educazione**. Le loro attività si sono poi estese anche a **Europa**, **America** e altre regioni.**APT34** utilizza diversi vettori d'attacco: **spearphishing** tramite email con allegati **Excel infetti**, **social engineering**, **vulnerabilità zero-day** (come **CVE-2017-0199** e **CVE-2017-11882**), **siti web fasulli** e **web shell** per mantenere l'accesso alle reti compromesse. Il gruppo fa uso di numerosi **malware personalizzati**, tra cui **Quadagent**, **Twoface**, **Helminth**, **OopsIE**, e altri.L'obiettivo principale di **APT34** è lo **spionaggio informatico** a beneficio degli interessi **strategici** e **geopolitici** iraniani, puntando alla raccolta di **informazioni sensibili** e **credenziali**, soprattutto da organizzazioni legate a governi rivali o infrastrutture critiche.Il report elenca inoltre vari **Indicatori di Compromissione (IoC)** e suggerisce misure difensive per le organizzazioni, sottolineando la necessità di un **approccio di sicurezza multilivello** poiché anche soluzioni **antivirus aggiornate** non garantiscono piena protezione contro minacce di questo tipo.

4.2 Analisi Vulnerabilita'

Nel corso dell'analisi di questo report sono state identificate le seguenti vulnerabilita':

Campo	Valore
cve	CVE-2017-0199
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-04-12T14:59Z
epss	0.94366
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo)
cpe	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, 2016; Word, Word Viewer, Office Web Apps

La vulnerabilità **CVE-2017-0199** colpisce **Microsoft Office** (versioni **2007**, **2010**, **2013**, **2016**, **Word Viewer** e **Office Web Apps**) e consente attacchi tramite **file malevoli**, sfruttando un **difetto critico** (**CVSS 7.8**). È molto **nota** e **sfruttata**, con **exploit pubblici** e moduli **Metasploit** disponibili, ed è riconosciuta nei principali **database di sicurezza**. Il rischio di sfruttamento è **molto alto**.

Campo	Valore
cve	CVE-2017-11882
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-11-15T03:29Z
epss	0.94384
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-119: Improper Restriction of Operationsthe Bounds of a Memory Buffer
cpe	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, 2016

La vulnerabilità **CVE-2017-11882** interessa **Microsoft Office** (**2007**, **2010**, **2013**, **2016**) e riguarda una gestione errata della **memoria** che permette l'**esecuzione di codice dannoso**. Ha un rischio **alto** (**CVSS 7.8**), numerosi **exploit pubblici** e moduli **Metasploit** disponibili, ed è ampiamente **sfruttata**, con elevata probabilità di attacco secondo i principali **database di sicurezza**.

Le informazioni temporali relative ai CVE di APT34 The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations sono le seguenti :

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice remoto in Microsoft Office/WordPad (OLE), sfruttabile tramite documenti RTF o Word malevoli.
Divulgazione	Divulgata pubblicamente ad aprile 2017. Utilizzata da APT34 in campagne phishing contro enti israeliani e altri target prima del rilascio della patch.
Zero day?	Sì, la vulnerabilità è stata sfruttata come zero-day da APT34 poco prima della pubblicazione della patch da parte di Microsoft.
Patch	Microsoft ha pubblicato la patch MS17-027 l'11 aprile 2017.
Utilizzo nel malware	Utilizzata in attacchi mirati tramite email di spear phishing con allegati Word/RTF malevoli, prima e subito dopo la patch, per compromissioni in Medio Oriente e altri paesi.

Table 16: Informazioni temporali per CVE-2017-0199 (APT34)

Punto	**Dettaglio**
Tipo	Vulnerabilità di corruzione della memoria in Microsoft Office Equation Editor, che consente esecuzione di codice remoto.
Divulgazione	Divulgata pubblicamente a novembre 2017.
Zero day?	Sfruttata da APT34 immediatamente dopo la disclosure, ma non come vero zero-day (patch e info erano pubbliche).
Patch	Microsoft ha pubblicato la patch MS17-11882 il 14 novembre 2017.
Utilizzo nel malware	Utilizzata per campagne di spear phishing verso organizzazioni governative e infrastrutture critiche nella regione MENA, spesso tramite allegati Office.

Table 17: Informazioni temporali per CVE-2017-11882 (APT34)

4.3 TTP MITRE ATTCK

Le TTP che abbiamo rilevato sono le seguenti :

ID	Tactic	Technique	Sub-technique	Descrizione
001	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	MALICIOUS FILE (T1203.002)	I macro malevoli sono incorporati in file Microsoft Excel. Quando la vittima abilita le macro, viene eseguito codice dannoso.
002	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	POWERSHELL (T1059.001)	Utilizzo di PowerShell per eseguire script malevoli sul sistema vittima.
003	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Email di phishing vengono utilizzate per consegnare documenti Excel weaponizzati.
004	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	VISUAL BASIC (T1059.005)	All'apertura del documento Excel e abilitazione macro, vengono eseguiti script VBA (Visual Basic for Applications).
005	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	POWERSHELL (T1059.001)	PowerShell viene utilizzato per le sue capacità avanzate e integrazione con Windows.
006	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Email di phishing utilizzate per consegnare documenti Excel weaponizzati.

007	INITIAL ACCESS (TA0001)	APPLICATION LAYER PROTOCOL (T1071)	WEB PROTOCOLS (T1071.001)	Creazione e hosting di siti web falsi che imitano servizi legittimi (es. portale VPN Juniper, siti Oxford).
008	RESOURCE DEVELOPMENT (TA0042)	ACQUIRE INFRASTRUCTURE (T1583)	DOMAINS (T1583.001)	Registrazione di domini simili a quelli di organizzazioni reali (es. Oxford University) per dare autenticità ai siti fake.
009	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	—	Sfruttamento della vulnerabilità CVE-2017-0199 che permette esecuzione di codice remoto tramite OLE in Windows.
010	PERSISTENCE (TA0003)	SERVER SOFTWARE COMPONENT (T1505)	WEB SHELL (T1505.003)	Utilizzo di webshell (TwoFace, RunningBee, RGDoor, ecc.) per ottenere persistenza su web server compromessi.
011	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	Il trojan “Agent Injector” viene eseguito tramite allegato email e installa la backdoor ISMAgent.
012	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Email di spear-phishing con oggetto “Important Issue” consegnano il trojan “Agent Injector”.
013	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	—	Sfruttamento della vulnerabilità CVE-2017-11882 in Microsoft Office Equation Editor per RCE.
014	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	Documento “ThreeDollars” utilizzato come delivery per il trojan OopsIE.

015	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di spear-phishing email a diversi destinatari della stessa organizzazione.
016	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Email di spear-phishing con allegati malevoli per consegnare malware.
017	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Il malware viene distribuito tramite documento Excel con macro malevoli.
018	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	WEB PROTOCOLS (T1071.001)	Il RAT comunica via HTTP per scambiare comandi o esfiltrare dati.
019	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	DNS (T1071.004)	Il RAT utilizza anche DNS per comunicazione, mascherando il traffico.
020	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Impersonificazione di un docente Cambridge su LinkedIn per convincere le vittime ad aprire link malevoli.
021	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	Esecuzione da parte dell'utente di un documento malevolo ricevuto tramite social engineering.
022	COMMAND AND CONTROL (TA0011)	ENCRYPTED CHANNEL (T1573)	—	Utilizzo di RAT per canali C2 con comunicazione HTTP/DNS potenzialmente cifrata.

023	DEFENSE EVASION (TA0005), PERSISTENCE (TA0003), PRIVILEGE ESCALATION (TA0004), INITIAL ACCESS (TA0001)	VALID ACCOUNTS (T1078)	—	Uso di account validi e tool come Twoface per harvesting credenziali e movimento laterale.
024	RECONNAISSANCE (TA0043)	GATHER VICTIM IDENTITY INFORMATION (T1589)	CREDENTIALS (T1589.001)	Raccolta di credenziali della vittima per futuri attacchi (es. con tool Pickpocket).

4.4 Tool Utilizzati

Table 19: Principali tool utilizzati:

Tool	**ID MITRE**	**Descrizione**
TwoFace	S0194	Web shell usata per harvesting credenziali e accesso persistente a server web compromessi, spesso insieme a varianti come RunningBee, RGDoor, HighShell, HyperShell.
RunningBee	—	Web shell utilizzata come payload di TwoFace per accesso remoto e mantenimento della persistenza su server IIS.

Tool	**ID MITRE**	**Descrizione**
RGDoor	S0258	Backdoor per Microsoft IIS server, creata in C++, consente controllo remoto e persistence.
Powruner	—	Backdoor PowerShell utilizzata per esecuzione comandi e controllo a distanza.
Helminth	S0170	Trojan Windows sviluppato ad hoc da APT34 per accesso remoto, esfiltrazione e comando.
OopsIE	S0264	Trojan distribuito via spear-phishing, impiegato per raccolta dati, persistence e comando.
Karko!	—	Malware progettato per l'esecuzione remota di codice su host compromessi.
ISMAgent	S0189	Backdoor modulare, con tecniche anti-analisi e varianti usate in diverse campagne.
Pickpocket	—	Strumento per il furto di credenziali dal browser e dal sistema Windows.
ValueVault	—	Tool usato per estrarre e visualizzare credenziali memorizzate nel Windows Vault.
LongWatch	—	Variante di Pickpocket per furto di credenziali dai browser.
PhpSpy	—	Backdoor PHP per ottenere foothold iniziale sulla rete bersaglio.
QuadAgent	—	Backdoor PowerShell, attribuita a campagne recenti di APT34.
ThreeDollars	—	Documento weaponizzato usato come vettore di delivery in campagne spear-phishing.
Fox Panel	—	Tool di controllo e hacking collegato ad APT34.
HighShell	—	Payload basato su web shell (TwoFace) per persistenza su server web.
Webmask	—	Script e tool per attacchi di DNS hijacking.
HyperShell	—	Loader di TwoFace per installare/persist web shell su target compromessi.

4.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
Microsoft Windows	Sistema Operativo	Vulnerabilità di esecuzione di codice tramite file malevoli (Excel, Office, eseguibili), incluso abuso di macro e scripting PowerShell. Sfruttate vulnerabilità come CVE-2017-0199 (OLE) per RCE su sistemi Windows.
Microsoft Office (Word, Excel)	Applicazione	Exploit di macro malevoli e vulnerabilità (es. CVE-2017-0199, CVE-2017-11882 Equation Editor), usati per esecuzione codice da allegati email weaponizzati (phishing/spearphishing).
Microsoft IIS	Server Web	Abuso di vulnerabilità e installazione di webshell custom (TwoFace, RGDoor, RunningBee, HyperShell) per ottenere persistenza su server compromessi.
Browser (Internet Explorer, Chrome)	Applicazione	Furto credenziali tramite tool come Pickpocket e LongWatch, sfruttando memorizzazione password locali.
Windows Vault	Sistema Operativo	Estrazione e furto di credenziali salvate tramite tool ValueVault.

Table 20: Principali prodotti vulnerabili sfruttati dal gruppo APT34

4.6 IoC

Gli **Indicators of Compromise** (**IoC**) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del **report originale**, all'interno dell'**appendice**. In questa sezione finale del **PDF**(pagine 13-24)è possibile trovare es-

empi di **hash**, **nomi di file**, **URL** malevoli, **domini** di **command and control**, **percorsi di debug** e altri indicatori tecnici associati alle varie famiglie di **malware** descritte nel rapporto.

4.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, ‘e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell’attacco:

Fase	**Tool suggerito**	**Note operative**
Simulazione spear-phishing	GoPhish	Invio di email di phishing con allegati Excel/Word weaponizzati (macro, exploit), creazione di link malevoli, raccolta dati su aperture/click.
Generazione documenti malevoli	Metasploit	Creazione di documenti Excel/Word con macro malevole, DDE, OLE, payload Powershell/VBA, oppure exploit (CVE) via Metasploit.
Esecuzione del payload	Nishang	Uso di macro/script Powershell/VBA per eseguire codice malevolo quando l'utente apre il documento weaponizzato. Nishang offre diversi payload Powershell pronti.
Persistence	Nishang, Empire	Persistenza su host compromessi tramite script Powershell (Nishang), Empire (agente C2 con funzioni di persistence) o via webshell. EvilWinRM per persistence su Windows Remoting.
Movimento laterale e harvesting credenziali	Mimikatz	Uso di CrackMapExec per movimento laterale e dump credenziali, LaZagne per furto password locali, Mimikatz (solo in lab) per test di credential dumping.
Command and Control (C2)	Covenant	Framework C2 open source con agenti Powershell e Python; supportano canali HTTP/S, comunicazioni cifrate, tasking, download/upload dati, exfiltrazione.
Evasione	Veil	Offuscamento script, payload fileless, generazione di shellcode e tecniche di bypass per evadere EDR/antivirus nei test di laboratorio.
Exfiltration	Rclone, Covenant	Esfiltrazione dati tramite upload su storage cloud (Rclone verso Nextcloud/-GoogleDrive), o download/upload da framework C2 (Covenant/Empire), script Powershell custom.

5 APT Fin6

Introduzione

FIN6 è un **gruppo APT** (Advanced Persistent Threat) specializzato principalmente in **attacchi finanziari** contro grandi aziende, con particolare attenzione al settore **retail** e ai servizi di **pagamento elettronico**. Attivo dal 2015, FIN6 è noto per la sua capacità di compromettere **sistemi POS** (Point of Sale) e rubare **dati di carte di pagamento** tramite sofisticate campagne di **phishing**, tecniche di **lateral movement** e l'utilizzo di **malware custom**. Le informazioni sottratte vengono poi rivendute nel **dark web**, generando profitti significativi per il gruppo. FIN6 si distingue per l'elevato livello di **professionalità**, l'approccio **mirato** e la costante evoluzione delle proprie tecniche di attacco.

5.1 More eggs Backdoor

Il report analizza una serie di campagne di **phishing** sofisticate, condotte a partire dalla metà del 2018 e attribuite a **FIN6** (identificato per l'uso della backdoor **More_eggs**). Queste campagne hanno preso di mira principalmente aziende statunitensi nei settori **retail**, **entertainment** e **pharma**. L'elemento centrale è la diffusione della backdoor **More_eggs** attraverso **offerte di lavoro fasulle**. Gli attaccanti sfruttano servizi di messaggistica legittimi come **LinkedIn** per avviare il primo contatto, utilizzando **profili falsi** e inviando richieste di collegamento. Successivamente, seguono **email personalizzate** che fanno riferimento al contatto precedente, rafforzando la credibilità dell'offerta. Queste email contengono spesso **link** a **siti web fake** che imitano agenzie di selezione, oppure **allegati dannosi** (**PDF**, **Word con macro**) progettati per infettare il sistema. Il **payload** finale, **More_eggs**, viene scaricato tramite queste macro o tramite loader **JScript** intermedi, e una volta eseguito consente agli attaccanti di **profilare** la vittima, raccogliere informazioni e scaricare ulteriori malware. Il report evidenzia come il gruppo cambi frequentemente le **tecniche di delivery** sfruttando builder (**Taurus Builder**, **VenomKit**) ottenuti in ambienti underground. Viene inoltre sottolineata la tendenza crescente a preferire campagne **mirate** e basate su **social engineering** avanzato, abbandonando i vecchi attacchi massivi "spray and pray". Infine, viene documentata la sovrapposizione con altre campagne (ad esempio contro **anti-money laundering offi-**

cer) e sono forniti **indicatori di compromissione** (**IOC**) utili per la detection.

5.2 Analisi Vulnerabilita‘

Nel corso dell'analisi di questo report sono state identificate le seguenti **vulnerabilità**:

Campo	Valore
cve	CVE-2017-0199
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-04-12T14:59Z
epss	0.94366
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Office (Word, Excel, PowerPoint) 2007/2010/2013/2016

La tabella riporta in modo strutturato tutte le informazioni principali relative alla vulnerabilità **CVE-2017-0199**. Sono elencati dettagli come il **punteggio CVSS** (7.8, quindi **gravità alta**), il **vettore di attacco**, la **data di pubblicazione** e i riferimenti all'esistenza di **exploit pubblici** sia su **ExploitDB** che su **Metasploit**. Si evidenzia inoltre che la vulnerabilità è stata inserita nelle liste di interesse di **CISA** e **VulnCheck**, e che sono disponibili **proof-of-concept** su **GitHub**. Tuttavia, nella sezione relativa alla classificazione **CWE**, non viene specificato un tipo di debolezza dettagliato, indicando

“**Insufficient Information**”.

Campo	Valore
cve	CVE-2017-8570
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-07-11T21:29Z
epss	0.94247
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	False
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Office (Word, Excel, PowerPoint) 2007/2010/2013/2016

La tabella mostra un **riepilogo dettagliato** delle principali informazioni riguardanti la vulnerabilità **CVE-2017-8570**, che interessa diverse versioni di **Microsoft Office** (**Word**, **Excel**, **PowerPoint** dal **2007** al **2016**). Vengono riportati dati come il **punteggio CVSS** pari a **7.8**, che indica una **gravità elevata**, insieme al **vettore di attacco** e alla **data di pubblicazione** della vulnerabilità. Sono inoltre specificate le fonti che confermano la presenza di **exploit pubblici** (**ExploitDB**, **PoC** su **GitHub**) e la rilevanza per enti come **CISA** e **VulnCheck**. Nonostante la gravità, la tabella segnala che non è stata associata una specifica categoria **CWE** dettagliata (“**Insufficient Information**”).

Campo	Valore
cve	CVE-2017-8759
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-09-13T01:29Z
epss	0.93893
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	False
nuclei	False
poc_github	True
cwe	CWE-94: Improper Control of Generation of Code ("Code Injection")
cpe	Microsoft .NET Framework 2.0/3.5/4.x (Running on/with Windows 7/8.1)

La tabella offre una **panoramica sintetica e completa** sulla vulnerabilità **CVE-2017-8759**, che riguarda il **Microsoft .NET Framework** (versioni **2.0**, **3.5** e **4.x**, in esecuzione su **Windows 7** e **8.1**). Sono elencate tutte le principali informazioni di **sicurezza**, tra cui il **punteggio CVSS** (7.8, **alto**), la **data di pubblicazione**, i riferimenti a fonti di **exploit pubblici** e la classificazione **CWE**, che in questo caso è "**Improper Control of Generation of Code (Code Injection)**". La tabella evidenzia inoltre che questa vulnerabilità è considerata rilevante da enti come **CISA** e **VulnCheck**, ed è oggetto di exploit pubblici su **ExploitDB** e **GitHub**. Complessivamente, il riepilogo risulta utile per valutare rapidamente **gravità**, **impatto** e **diffusione** degli exploit legati a questa vulnerabilità.

Campo	Valore
cve	CVE-2017-11882
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-11-15T03:29Z
epss	0.94384
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
cpe	Microsoft Office (2007/2010/2013/2016)

La tabella riassume tutte le **informazioni fondamentali** sulla vulnerabilità **CVE-2017-11882**, che interessa diverse versioni di **Microsoft Office** (**2007**, **2010**, **2013**, **2016**). Oltre ai dati identificativi come il **punteggio CVSS** pari a **7.8** (quindi **gravità alta**), vengono indicati i principali **vettori di attacco**, la **data di pubblicazione**, e la presenza di **exploit pubblici** su piattaforme come **ExploitDB**, **Metasploit** e **GitHub**. La vulnerabilità è inoltre classificata come rilevante da enti come **CISA** e **VulnCheck**. Dal punto di vista tecnico, è catalogata come **CWE-119** ("**Improper Restriction of Operations within the Bounds of a Memory Buffer**"), tipica dei **buffer overflow**.

Campo	Valore
cve	CVE-2018-0802
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2018-01-10T01:29Z
epss	0.94103
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	False
nuclei	False
poc_github	True
cwe	CWE-787: Out-of-bounds Write
cpe	Microsoft Office Equation Editor (2007/2010/2013/2016)

La tabella fornisce una **sintesi delle informazioni chiave** sulla vulnerabilità **CVE-2018-0802**, che riguarda il componente **Equation Editor** di **Microsoft Office** nelle versioni **2007**, **2010**, **2013** e **2016**. Viene riportato un **punteggio CVSS** di **7.8**, a indicare una **gravità alta**, insieme ai dettagli tecnici come il **vettore di attacco** e la **data di pubblicazione**. La vulnerabilità è riconosciuta da enti come **CISA** e **VulnCheck**, mentre non risultano **exploit pubblici** su **ExploitDB** e **Metasploit**, anche se è disponibile un **proof-of-concept** su **GitHub**. Dal punto di vista tecnico, si tratta di una vulnerabilità di tipo **Out-of-bounds Write** (**CWE-787**), tipica dei **buffer overflow**.

Campo	Valore
cve	CVE-2018-8174
cvss-bt_score	7.5
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.5
base_severity	HIGH
base_vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2018-05-09T19:29Z
epss	0.94283
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	False
nuclei	False
poc_github	True
cwe	CWE-787: Out-of-bounds Write
cpe	Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10 (1607/1703/1709/1803), Windows Server 2008 SP2, Server 2008 R2 SP1 (x64/Itanium), Server 2012, Server 2012 R2, Server 2016 (1709/1803)

La tabella presenta un **riepilogo dettagliato** della vulnerabilità **CVE-2018-8174**, nota anche come **"Double Kill"**, che ha interessato numerose versioni di sistemi operativi **Microsoft**, tra cui **Windows 7**, **8.1**, **10** (diverse build), e vari **Windows Server**. La **gravità** della vulnerabilità è **elevata**, con un **punteggio CVSS** di **7.5**, e viene identificata come un **Out-of-bounds Write** (**CWE-787**), una tipica vulnerabilità di **buffer overflow**. La tabella riporta tutte le principali **informazioni di sicurezza**, come i **vettori di attacco**, la **data di pubblicazione** e la presenza di **exploit pubblici** su **ExploitDB** e **GitHub**. Inoltre, evidenzia che la vulnerabilità è stata segnalata anche

da enti come **CISA** e **VulnCheck**, sottolineando la sua **importanza per la sicurezza**.

Le informazioni temporali relative alle CVE contenute in **More eggs Backdoor** sono le seguenti:

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice tramite file RTF e documenti Word che sfruttano l'Object Linking and Embedding (OLE) per scaricare ed eseguire script malevoli.
Divulgazione	Divulgata pubblicamente ad aprile 2017; exploit e PoC disponibili online nello stesso mese.
Zero day?	Non era più una zero day durante le campagne osservate: il malware colpiva sistemi non aggiornati.
Patch	Patch rilasciata da Microsoft con MS17-017 l'11 aprile 2017.
Utilizzo nel malware	Utilizzata dal gruppo per diffondere il payload More_eggs tramite documenti Word malevoli allegati a email di phishing.

Table 22: Dettagli temporali per CVE-2017-0199

Punto	**Dettaglio**
Tipo	Vulnerabilità di code execution via documenti Word (formato XML) che sfruttano l'esecuzione di contenuti embedded dannosi.
Divulgazione	Pubblicata a luglio 2017, con exploit e PoC disponibili online subito dopo la disclosure.
Zero day?	Non era più una zero day nelle campagne osservate, ma sfruttata su sistemi senza patch.
Patch	Patch distribuita da Microsoft l'11 luglio 2017 con MS17-054.
Utilizzo nel malware	Impiegata per l'esecuzione di codice e la delivery di More_eggs tramite allegati Word e link malevoli nelle email di spear phishing.

Table 23: Dettagli temporali per CVE-2017-8570

Punto	**Dettaglio**
Tipo	Vulnerabilità di code injection nella gestione di SOAP WSDL dalla libreria .NET Framework, sfruttabile tramite file RTF o Word appositamente creati.
Divulgazione	Divulgata e patchata pubblicamente a settembre 2017, con PoC pubblici subito disponibili.
Zero day?	Sfruttata solo dopo la disclosure; non utilizzata come zero day nelle campagne note.
Patch	Patch rilasciata da Microsoft il 12 settembre 2017.
Utilizzo nel malware	Utilizzata per l'esecuzione di codice remoto in allegati malevoli, all'interno delle campagne di spear phishing analizzate nel report.

Table 24: Dettagli temporali per CVE-2017-8759

Punto	**Dettaglio**
Tipo	Vulnerabilità di buffer overflow nell'Equation Editor di Microsoft Office che consente l'esecuzione di codice arbitrario.
Divulgazione	Divulgata pubblicamente e patchata a novembre 2017, con exploit pubblici poco dopo.
Zero day?	Non era più zero day durante l'uso nelle campagne More_eggs.
Patch	Patch rilasciata da Microsoft il 14 novembre 2017.
Utilizzo nel malware	Sfruttata da allegati malevoli (.doc, .rtf) per ottenere esecuzione di codice remoto durante le campagne di phishing descritte nel report.

Table 25: Dettagli temporali per CVE-2017-11882

Punto	**Dettaglio**
Tipo	Vulnerabilità di tipo buffer overflow nell'Equation Editor di Office, simile a CVE-2017-11882.
Divulgazione	Pubblicata e patchata a gennaio 2018, con exploit pubblici successivi.
Zero day?	Non zero day al momento delle campagne More_eggs; sfruttata su host non aggiornati.
Patch	Patch rilasciata da Microsoft il 9 gennaio 2018.
Utilizzo nel malware	Utilizzata per consentire l'esecuzione di codice arbitrario tramite allegati Office nelle email di spear phishing.

Table 26: Dettagli temporali per CVE-2018-0802

Punto	Dettaglio
Tipo	Vulnerabilità di tipo “out-of-bounds write” nel motore VBScript di Windows, sfruttabile tramite documenti Office o pagine web malevole.
Divulgazione	Rivelata pubblicamente a maggio 2018; exploit e PoC disponibili poco dopo la disclosure.
Zero day?	Non più zero day nelle campagne More_eggs; sfruttata su sistemi non patchati.
Patch	Patch pubblicata da Microsoft l’8 maggio 2018.
Utilizzo nel malware	Utilizzata per eseguire codice remoto nei sistemi delle vittime, sempre tramite spear phishing.

Table 27: Dettagli temporali per CVE-2018-8174

5.3 TTP MITRE ATTCK

Le TTP che abbiamo rilevato sono le seguenti:

ID	Tactic	Technique	Sub-technique	Descrizione
001	RECONNAISSANCE (TA0043)	GATHER VICTIM IDENTITY INFORMATION (T1589)	—	Gli avversari raccolgono informazioni sull’identità delle vittime, come nomi dei dipendenti e indirizzi email, utili per il targeting.
002	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Invio di email di spear phishing con link malevolo per ottenere accesso ai sistemi delle vittime.
003	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di email di spear phishing con allegato malevolo per compromettere la vittima.

004	COMMAND AND CONTROL (TA0011)	INGRESS TOOL TRANSFER (T1105)	—	Trasferimento di strumenti o file da un sistema controllato dagli avversari verso la rete della vittima tramite canali di comando e controllo.
005	EXECUTION (TA0002)	USER EXECUTION (T1204)	MALICIOUS FILE (T1204.002)	L'avversario convince l'utente ad aprire un file malevolo tramite social engineering, portando all'esecuzione di codice. Tool: Taurus Builder, VenomKit.
006	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	JAVASCRIPT (T1059.007)	Gli avversari abusano di implementazioni JavaScript per eseguire codice sul sistema compromesso.
007	COMMAND AND CONTROL (TA0011)	INGRESS TOOL TRANSFER (T1105)	—	Utilizzo di More_eggs (S0284) per trasferire file o strumenti all'interno della rete della vittima tramite C2.
008	COLLECTION (TA0009)	DATA FROM LOCAL SYSTEM (T1005)	—	Gli avversari raccolgono dati dal sistema locale tramite il malware More_eggs (S0284).

5.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti. Di seguito sono riportati gli strumenti:

Tool	ID MITRE	Descrizione
Taurus Builder	—	Tool acquistato in forum underground, utilizzato per la creazione di documenti malevoli (ad esempio, documenti Word con macro dannose) che sfruttano varie vulnerabilità di Office. Utilizza il bypass CMSTP per aggirare alcune protezioni.
VenomKit	—	Builder per la generazione di documenti malevoli che sfruttano diverse vulnerabilità di Microsoft Office (tra cui CVE-2017-0199, CVE-2017-8570, CVE-2017-8759, CVE-2017-11882, CVE-2018-0802 e CVE-2018-8174). Impiega anch'esso il bypass CMSTP per aumentare la probabilità di successo.
More_eggs	S0284	Malware scritto in JScript, utilizzato sia come downloader che per la raccolta di informazioni sulla macchina compromessa. Permette di scaricare payload aggiuntivi, eseguire comandi e profilare il sistema infetto.

Table 29: Tool utilizzati nelle campagne More_eggs

5.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	Tipologia	Note sulla vulnerabilità
Microsoft Office (Word, Excel, PowerPoint, Equation Editor)	Applicazione	Vulnerabilità di esecuzione di codice remoto tramite documenti malevoli (RTF, DOCX, macro, embedded objects). Le campagne sfruttavano diverse CVE: CVE-2017-0199, CVE-2017-8570, CVE-2017-8759, CVE-2017-11882, CVE-2018-0802, CVE-2018-8174, spesso tramite allegati email o link a landing page.
Microsoft Windows	Sistema Operativo	Sistema target delle infezioni: vulnerabile alle tecniche di social engineering tramite file Office, PDF o eseguibili. Le campagne puntavano a workstation Windows di aziende nei settori retail, entertainment e pharma.

Table 30: Prodotti vulnerabili More_eggs

5.6 IoC

Gli *Indicators of Compromise* (IoC) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del report originale (Pag. 7 e 8). In questa sezione finale del PDF è possibile trovare esempi di hash, nomi di file, URL malevoli, domini di command and control, e altri indicatori tecnici associati alle varie famiglie di malware descritte nel rapporto.

5.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, 'e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell'attacco:

Fase	**Tool suggerito**	**Note operative**
Generazione documenti malevoli (Word/PDF)	Metasploit, Taurus Builder	Creazione di file Office (DOC/RTF) e PDF con macro, exploit e payload personalizzati per simulare vulnerabilità reali (es. CVE-2017-0199, CVE-2017-8570, ecc.).
Hosting landing page malevole	Apache, Nginx	Simulazione di siti clone o pagine di recruiting compromesse per l'hosting e il download dei documenti infetti.
Payload/JScript downloader	Metasploit	Esecuzione e gestione di script di download payload, dropper e loader JScript per simulare la seconda fase dell'infezione.
Accesso remoto e C2	Metasploit	Gestione delle sessioni di controllo remoto, raccolta informazioni sul sistema e comando dei payload.
Raccolta dati, profiling sistema	Metasploit post modules	Raccolta dati di sistema, informazioni utenti, enumerazione processi e network per simulare le azioni post-infezione del malware More_eggs.
Persistenza e movimento laterale	Metasploit	Installazione di persistence, simulazione di movimenti laterali su target Windows interni.
Esfiltrazione dati	Metasploit	Download/esfiltrazione di file sensibili, documenti e credenziali dal sistema compromesso.

Table 31: Simulazione delle principali fasi di attacco della campagna More_eggs/FIN6

6 APT Fin7

Introduzione

APT Fin7, noto anche come **Carbanak Group**, **Navigator Group** o **Gold Niagara**, è un gruppo **cybercriminale avanzato** con motivazioni principalmente **finanziarie**, attivo almeno dal **2015**. Sebbene inizialmente confuso con APT di tipo statale, è ora classificato come uno degli attori più sofisticati nel panorama del **cybercrime**, con legami documentati con altre organizzazioni come **REvil** e **Black Basta**. I suoi **obiettivi principali** includono **istituti finanziari**, **catene di ristorazione**, **aziende di logistica**, **assicurazioni** e **infrastrutture critiche**. Fin7 è responsabile di numerose campagne contro oltre **100 aziende in tutto il mondo**, provocando centinaia di milioni di dollari di perdite economiche.
Le **tecniche utilizzate** dal gruppo includono **spear phishing mirato** con allegati dannosi in formato **RTF** o **LNK**, uso di **malware complessi** come **Carbanak**, **GRIM SPIDER**, **BOOSTWRITE** e **IceID**, e l'implementazione di **backdoor custom** che consentono il controllo remoto persistente. Una delle caratteristiche distintive di Fin7 è la sua **struttura pseudo-aziendale**, che si avvale di false società di sicurezza informatica (*es. Combi Security*) per reclutare sviluppatori e analisti inconsapevoli. Inoltre, il gruppo è noto per l'uso di **strumenti legittimi** come `PowerShell`, `Metasploit`, e `Cobalt Strike` per eludere i controlli di sicurezza e muoversi lateralmente nei sistemi infetti.
Le sue **caratteristiche principali** includono una notevole **resilienza operativa**, **adattabilità nelle tattiche** e una **capacità tecnica elevata**, che lo rendono uno degli attori criminali più pericolosi e difficili da attribuire e neutralizzare.
Tra i vari report su Fin7 abbiamo analizzato quello che ci forniva il maggior numero di informazioni operative e tecniche.

6.1 Profile of an Adversary - FIN7_Deepwatch

Il report è un'analisi approfondita delle operazioni del gruppo **cybercriminale FIN7**, attivo almeno dal **2015** e noto per aver condotto **campagne globali** a scopo **finanziario**, principalmente contro aziende dei settori **retail**, **ristorazione**, **ospitalità**, **sanitario**

e **logistica**. Sebbene non affiliato direttamente ad apparati statali, il livello di **sofisticazione tecnica**, **organizzazione interna** e **persistence** lo rende comparabile ad attori APT sponsorizzati da stati.

Il documento analizza le principali **tattiche**, **tecniche** e **procedure** (TTPs) utilizzate dal gruppo, tra cui campagne di **spear-phishing** con allegati **LNK** o **DOC**, e l'impiego di **malware custom** come **Carbanak**, **GrimAgent**, **Tirion Loader**, **PowerTrick**, e **Boostwrite**. Viene messa in luce anche la capacità di **aggirare i controlli di sicurezza** sfruttando strumenti legittimi come `PowerShell`, `RDP` e `Cobalt Strike` per movimenti laterali e **escalation di privilegi**.

Il **modus operandi** di FIN7 include l'iniziale compromissione tramite social engineering e allegati malevoli, seguita da una fase di **ricognizione interna** e successivo **esfiltramento dei dati**, oltre all'eventuale **distribuzione di ransomware** in collaborazione con altri gruppi. Il report evidenzia anche l'uso di una **falsa struttura aziendale** (come *Combi Security*) per reclutare sviluppatori inconsapevoli e mantenere una parvenza di legalità.

Il report sottolinea infine l'elevata **resilienza**, **adattabilità** e **persistenza** del gruppo, capace di modificare rapidamente i propri strumenti per **evitare il rilevamento**, e continuare ad operare anche dopo arresti o compromissioni pubbliche.

6.2 Analisi Vulnerabilità

Nel corso dell'analisi di questo report sono state identificate le seguenti vulnerabilità:

Campo	Valore
cve	CVE-2015-2545
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2015-09-09T00:59Z
epss	0.93252
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	False
nuclei	False
poc_github	False
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Office 2007/2010/2013 (SP)

La vulnerabilità CVE-2015-2545 interessa varie versioni di Microsoft Office (2007, 2010, 2013 con Service Pack) e consente a un attaccante locale, tramite un file appositamente predisposto, di eseguire codice arbitrario con alti privilegi. È classificata come grave, con un punteggio CVSS di 7.8, e riconosciuta da Microsoft. Pur non essendo disponibili exploit pubblici su ExploitDB o Metasploit, il rischio di sfruttamento è elevato (EPSS 0.93). La vulnerabilità figura nei database CISA KEV e VulnCheck KEV e riguarda una convalida impropria degli input (CWE-20).

Campo	Valore
cve	CVE-2015-1701
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2015-04-21T10:59Z
epss	0.90769
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Windows Vista/Server 2008/Server 2003

La vulnerabilità CVE-2015-1701 affligge alcuni sistemi operativi Windows (Vista, Server 2008, Server 2003) e consente a un utente locale di elevare i propri privilegi a causa di un errore nei controlli di accesso. È classificata come grave, con un punteggio CVSS di 7.8, ed è ben documentata da Microsoft. Sono disponibili exploit pubblici, moduli per Metasploit e proof-of-concept su GitHub, mentre il rischio di sfruttamento è elevato (EPSS 0.90). È inclusa nei database CISA KEV e VulnCheck KEV, e riguarda i permessi e privilegi del sistema operativo (CWE-264).

Campo	Valore
cve	CVE-2017-0199
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	7.8
base_severity	HIGH
base_vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
assigner	secure@microsoft.com
published_date	2017-04-12T14:59Z
epss	0.94366
cisa_kev	True
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Office 2007/2010/2013/2016

La vulnerabilità CVE-2017-0199 colpisce Microsoft Office (2007, 2010, 2013, 2016) e WordPad in diverse versioni di Windows (da Vista a 8.1). Un file RTF o documento Word contenente un oggetto OLE malevolo può portare all'esecuzione remota di codice. È classificata come grave, con un punteggio CVSS di 7.8, ed è ampiamente conosciuta e sfruttata. Sono disponibili exploit pubblici, moduli Metasploit e PoC su GitHub. Il rischio di sfruttamento è molto alto (EPSS 0.94). La vulnerabilità compare nei database CISA KEV e VulnCheck KEV e riguarda la generazione non sicura di codice (CWE-94). Le informazioni temporali relative a **Profile of an Adversary - FIN7_Deepwatch** sono le seguenti:

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice arbitrario in Microsoft Office tramite gestione errata di file EPS.
Divulgazione	Divulgata pubblicamente nel settembre 2015.
Zero day?	Non risulta sfruttata come zero-day.
Patch	Microsoft ha rilasciato una patch tramite aggiornamento di sicurezza MS15-099 pubblicato il 9 settembre 2015.
Utilizzo nel malware	Utilizzata da FIN7 in campagne di spear-phishing tramite allegati Office contenenti exploit.

Table 32: Dettagli temporali per CVE-2015-2545

Punto	**Dettaglio**
Tipo	Vulnerabilità di escalation dei privilegi in Windows Kernel (win32k.sys).
Divulgazione	Divulgata pubblicamente nell'aprile 2015.
Zero day?	Non risultano campagne attribuite a FIN7 che l'abbiano sfruttata come zero-day.
Patch	Microsoft ha rilasciato una patch tramite aggiornamento di sicurezza MS15-051 il 14 aprile 2015.
Utilizzo nel malware	Utilizzata da FIN7 in catene d'attacco post-exploitation.

Table 33: Dettagli temporali per CVE-2015-1701

Punto	Dettaglio
Tipo	Vulnerabilità di esecuzione remota di codice in Microsoft Office e WordPad tramite oggetti OLE in RTF.
Divulgazione	Scoperta e divulgata ad aprile 2017; attivamente sfruttata prima della disclosure.
Zero day?	Non risulta sfruttata come zero-day da FIN7 secondo quanto riportato dal documento.
Patch	Microsoft ha rilasciato una patch il 11 aprile 2017 tramite aggiornamento MS17-010.
Utilizzo nel malware	Utilizzata da FIN7 per eseguire codice arbitrario tramite allegati Office in campagne di spear-phishing.

Table 34: Dettagli temporali per CVE-2017-0199

6.3 TTP MITRE ATT&CK

Le TTP che abbiamo rilevato sono le seguenti :

ID	Tactic	Technique	Sub-technique	Descrizione
001	INITIAL ACCESS (TA0001)	PHISHING (T1566)	—	FIN7 avvia gli attacchi con email di spear phishing che mirano a scatenare una reazione emotiva per indurre la vittima ad aprire allegati o link malevoli.
002	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di allegati nell'ambito di campagne spear phishing: il primo documento appare innocuo ma contiene sistemi di tracciamento delle aperture.

003	DISCOVERY (TA0007)	SYSTEM NETWORK CONNECTIONS DISCOVERY(T1016)	—	Il Documento o il meccanismo di tracciamento fornisce informazioni sulle connessioni di rete o sui dettagli del sistema.
004	EXECUTION (TA0002)	EXPLOITATION FOR CLIENT EXECUTION (T1203)	—	Sfruttamento di vulnerabilità in applicazioni client per eseguire codice malevolo sul sistema bersaglio.
005	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING ATTACHMENT (T1566.001)	Invio di email di phishing con allegati malevoli a individui selezionati per ottenere l'accesso iniziale.
006	EXECUTION (TA0002), PERSISTENCE (TA0003), PRIVILEGE ESCALATION (TA0004)	SCHEDULED TASK/JOB (T1053)	SCHEDULED TASK (T1053.005)	Creazione di task pianificati per garantire la persistenza e ristabilire le connessioni con i server C2.
009	DEFENSE EVASION (TA0005), PRIVILEGE ESCALATION (TA0004)	PROCESS INJECTION (T1055)	—	Iniezione di codice in processi legittimi per eludere i controlli basati sui processi e potenzialmente elevare i privilegi.

6.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti. Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
CARBANAK	S0030	Malware utilizzato per ottenere accesso remoto e persistente alle reti bancarie, usato da FIN7 per il furto di dati finanziari; include funzionalità di keylogging, screen capture, esecuzione comandi remoti, e movimenti laterali.
GRIZZLY STEPPE RAT	S0414	Tool impiegato per esfiltrazione e comando remoto; può comunicare con C&C via HTTP/S e consente operazioni furtive su sistemi compromessi. Utilizzato in alcune operazioni ricondotte a FIN7.
POWERSPLIT	S0373	Strumento PowerShell usato da FIN7 per eseguire comandi da remoto e interagire con il sistema target tramite interpreti di script e comandi.
GHOST RAT	S0032	Remote Access Trojan (RAT) usato per sorveglianza e controllo remoto del sistema. Può registrare input, rubare file e scattare screenshot. Alcuni cluster attribuiti a FIN7 hanno impiegato questo RAT.
SQLRAT	S0380	Tool basato su SQL Server utilizzato per eseguire script malevoli, spesso impiegato in ambienti Windows compromessi. FIN7 l'ha usato per mantenere accesso e lanciare comandi SQL.

Tool	ID MITRE	Descrizione
CARAMBA	S1015	Backdoor impiegata da FIN7 in campagne mirate. Fornisce controllo remoto del sistema e possibilità di caricare/eseguire altri payload.
JSSLoader	S1046	Downloader scritto in .NET utilizzato da FIN7 per ottenere payload aggiuntivi. È spesso distribuito tramite email di spearphishing.
Lizar	S1070	Framework modulare con capacità di esecuzione comandi, movimenti laterali, e raccolta credenziali. Utilizzato da FIN7 in fasi post-compromissione.

Table 36: Tool associati al gruppo FIN7

6.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
Microsoft Windows	Sistema Operativo	Sfruttato per vulnerabilità di esecuzione di codice remoto e privilege escalation. FIN7 ha utilizzato exploit come CVE-2017-0199 (via documenti Office) e abusi di strumenti Windows legittimi (es. PowerShell, WMI, schtasks).
Microsoft Office	Applicazione	Spesso vettore iniziale via spearphishing con documenti malevoli contenenti macro o exploit come CVE-2017-0199 e CVE-2018-0802, che consentono esecuzione remota di codice senza interazione dell'utente.
POS Systems (vari vendor)	Hardware/ Software	Target primario di FIN7 per il furto di dati di pagamento. Exploit e backdoor installati per l'intercettazione delle transazioni in memoria (RAM scraping).
JavaScript Engines	Runtime	Utilizzato in attacchi basati su payload JavaScript offuscati all'interno di documenti HTML o JS inviati via email; può comportare esecuzione arbitraria nel browser o via interpreti embedded.
Remote Desktop Protocol (RDP)	Servizio di rete	In alcuni casi FIN7 ha sfruttato RDP esposto pubblicamente con credenziali deboli o rubate per movimenti laterali e persistenza, senza necessità di exploit software.
SQL Server	Database	Targetato in fase post-exploitation per movimenti laterali o esecuzione di comandi tramite SQL RAT; sfruttamento di configurazioni deboli o credenziali statiche.

Table 37: Prodotti vulnerabili

6.6 IoC

Gli *Indicators of Compromise* (IoC) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del report originale (Pag. 8-12). In questa sezione finale del PDF è possibile trovare esempi di hash, nomi di file, URL malevoli, domini di command and control, e altri indicatori tecnici associati alle varie famiglie di malware descritte nel rapporto

6.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, 'e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell'attacco:

Fase	**Tool suggerito**	**Note operative**
Simulazione spear-phishing	GoPhish	Invio di email mirate contenenti allegati o link malevoli. Utile per testare la resilienza degli utenti a campagne simili a quelle condotte da FIN7.
Generazione documenti malevoli	Metasploit	Creazione di documenti Office (doc, docm) con macro VBA o exploit (es. CVE-2017-0199) per simulare vettori iniziali d'infezione.
Accesso iniziale / Payload delivery	Metasploit	Deploy di stager tramite macro nei documenti allegati. Setup di listener e C2 per gestire l'infezione.
Privilege escalation	Metasploit (local exploit)	Ricognizione dei privilegi sul sistema e sfruttamento di vulnerabilità locali per elevare i privilegi (es. token impersonation o exploit LPE).
Credential dumping	Mimikatz	Estrazione di hash, password in chiaro, e credenziali da LSASS e altri store locali.

Fase	Tool suggerito	Note operative
Movimento laterale	PsExec, RDP	Utilizzo di credenziali rubate per accedere ad altri host nella rete tramite servizi remoti.
Persistenza	Registry RunKeys, Scheduled Tasks	Installazione di persistence (fileless o tramite backdoor), utilizzando task pianificati o chiavi di registro.
C2 e controllo remoto	Metasploit	Gestione interattiva dei target compromessi tramite beacon o agent. Comunicazione HTTP/HTTPS simile a quella usata da FIN7.
Esfiltrazione dati	Rclone, Metasploit	Simulazione di furto di file sensibili, upload verso cloud o esfiltrazione tramite DNS tunneling.
Simulazione attacchi DoS (impatto)	Hping3, Slowloris, Metasploit auxiliary	Simulazione di attività distruttive (opzionali per FIN7) su sistemi bersaglio controllati in laboratorio.

Table 38: Tool consigliati per la simulazione in ambiente di laboratorio

7 APT Sandworm

Introduzione

APT Sandworm, noto anche come **TeleBots**, **Voodoo Bear** o **Iron Viking**, è un gruppo **cybermilitare avanzato** presumibilmente legato all'intelligence militare russa, attivo almeno dal **2010**. È considerato uno degli attori più temuti nel panorama delle minacce informatiche di tipo statale, con una chiara agenda geopolitica e militare. Sandworm è noto per aver condotto attacchi sofisticati e distruttivi contro **infrastrutture critiche**, **enti governativi**, **organizzazioni di sicurezza** e **società energetiche** in Europa e Nord America, con particolare attenzione all'Europa orientale e all'Ucraina.

Le **tecniche utilizzate** dal gruppo comprendono **spear phishing mirato** con allegati malevoli in formato **Word** o **Excel** contenenti macro dannose, l'uso di **malware sofisticati** come **BlackEnergy**, **Industroyer/CrashOverride**, **NotPetya**, e **Cyclops Blink**, e l'implementazione di **backdoor custom** e **wiper** per causare interruzioni operative gravi e permanenti. Sandworm sfrutta inoltre **strumenti legittimi** come `PowerShell` e `Cobalt Strike` per mantenere la persistenza e muoversi lateralmente nei network compromessi. Le operazioni di Sandworm sono spesso caratterizzate da una profonda conoscenza delle infrastrutture industriali e dei sistemi di controllo ICS/SCADA.
Le sue **caratteristiche principali** includono un elevato livello di **coordinamento militare**, **capacità tecnica avanzata** e una propensione all'uso di **tattiche distruttive** e **cyber sabotaggi**, rendendolo uno dei gruppi APT più pericolosi e difficili da contrastare a livello globale. Le sue campagne hanno avuto impatti significativi su reti elettriche, sistemi di comunicazione e infrastrutture critiche, rappresentando una minaccia costante alla sicurezza nazionale di numerosi paesi.
Tra i vari report su **sandworm** abbiamo analizzato quello che ci forniva il maggior numero di informazioni operative e tecniche.

7.1 CrashOverride

Il **report CrashOverride** è un'analisi approfondita delle operazioni del gruppo che ha utilizzato tecniche di **cyber sabotaggio** mirate contro **infrastrutture critiche**, in particolare **sistemi di controllo industriale** (ICS) nel settore energetico, con attacchi documentati a partire dal **2016**. Il report evidenzia l'impatto devastante di tali operazioni, come l'interruzione di forniture elettriche su larga scala, con particolare attenzione agli eventi in Ucraina.
Il documento descrive l'impiego di tecniche sofisticate che coinvolgono protocolli ICS specifici, consentendo al gruppo di interagire direttamente con dispositivi di controllo industriale quali **relay elettrici** e **sistemi SCADA**. Vengono analizzate le modalità con cui sono state create **backdoor** per garantire persistenza e controllo remoto, la capacità di cancellare log, nonché l'integrazione con altri strumenti malevoli come **BlackEnergy**.
Le tattiche descritte nel report includono fasi di **spear phishing**, compromissioni di rete preesistenti, **ricognizione interna** e **movimenti laterali** volti a identificare i sistemi ICS critici. Le azioni culminano in attacchi mirati che provocano **disabilitazioni tem-**

poranee o permanenti di componenti infrastrutturali fondamentali, con l'obiettivo di causare danni fisici e interruzioni di servizio significative.

Il report sottolinea come la natura altamente specializzata e il potenziale distruttivo delle operazioni analizzate rendano CrashOverride uno dei casi più significativi di **cyber sabotaggio** contro infrastrutture critiche, con importanti implicazioni per la sicurezza nazionale e la resilienza dei sistemi energetici.

7.2 Analisi Vulnerabilità

Nel corso dell'analisi di questo report è stata identificata la seguente vulnerabilità:

Campo	Valore
cve	CVE-2015-5374
cvss-bt_score	7.8
cvss-bt_severity	HIGH
cvss-bt_vector	AV:N/AC:L/Au:N/C:N/I:N/A:C/E:H
cvss_version	2.0
base_score	7.8
base_severity	HIGH
base_vector	AV:N/AC:L/Au:N/C:N/I:N/A:C
assigner	cve@mitre.org
published_date	2015-07-18T10:59Z
epss	0.83908
cisa_kev	False
vulncheck_kev	True
exploitdb	True
metasploit	True
nuclei	False
poc_github	True
cwe	CWE-19: Data Processing Errors
cpe	libav (multimedia framework)

La tabella riportata sintetizza le informazioni chiave relative alla vulnerabilità **CVE-2015-5374**, classificata con un punteggio CVSS di **7.8** e severità **HIGH**. Questa vulnerabilità, nota come *Use After Free* (CWE-416), è stata pubblicata il **18 luglio 2015** e riguarda principalmente la libreria **libav**, un framework multimediale. La valutazione del rischio evidenzia un impatto significativo sulla disponibilità del sistema, mentre l'attacco

può essere eseguito da remoto senza autenticazione. Sono disponibili exploit pubblici e moduli Metasploit per questa vulnerabilità, indicando un elevato potenziale di sfruttamento. Nonostante non sia inclusa nella KEV di CISA, risulta presente in altri database di vulnerabilità e proof-of-concept su GitHub.
Le informazioni temporali relative a **CVE-2015-5374** sono le seguenti:

Punto	**Dettaglio**
Tipo	Vulnerabilità di tipo Use After Free in libav (framework multimediale), che può consentire esecuzione arbitraria di codice.
Divulgazione	Divulgata pubblicamente il 18 luglio 2015.
Zero day?	Non risulta sfruttata come zero-day.
Patch	Patch di sicurezza pubblicata da Siemens a luglio 2015.
Utilizzo nel malware	Il modulo SIPROTEC DoS di CrashOverride sfrutta la CVE-2015-5374 per mettere fuori uso i dispositivi di protezione, ampliando l'impatto sull'infrastruttura elettrica e facilitando ulteriori attacchi come l'islanding delle sottostazioni.

Table 39: Dettagli temporali per CVE-2015-5374

7.3 TTP MITRE ATT&CK

Le TTP che abbiamo rilevato sono le seguenti :

ID	**Tactic**	**Technique**	**Sub-technique**	**Descrizione**
001	IMPACT (TA0040)	DISK WIPE (T1561)	—	Gli avversari possono cancellare o corrompere i dati del disco su sistemi specifici o su larga scala per interrompere la disponibilità delle risorse di sistema e di rete.

002	IMPACT (TA0040)	FIRMWARE CORRUPTION (T1495)	—	Gli avversari possono sovrascrivere o corrompere la memoria flash del BIOS o di altri firmware, rendendo i dispositivi inoperabili o incapaci di avviarsi, negando così la disponibilità del sistema o dei dispositivi.
003	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	APPLICATION LAYER PROTOCOL: WEB PROTOCOLS (T1071.001)	Gli avversari possono comunicare usando protocolli del livello applicativo associati al traffico web per evitare il rilevamento e confondersi con il traffico esistente. Il backdoor apre un canale HTTP verso un C2 esterno tramite proxy interno.
004	PERSISTENCE (TA0003)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Gli avversari possono creare o modificare processi di sistema per eseguire ripetutamente payload malevoli come parte del meccanismo di persistenza.
005	COMMAND AND CONTROL (TA0011)	PROXY (T1090)	PROXY: INTERNAL PROXY (T1090.001)	Gli avversari possono usare un proxy per dirigere il traffico tra sistemi o come intermediario per le comunicazioni verso un C2, evitando connessioni dirette all'infrastruttura di comando. Il malware contatta un proxy locale hard-coded.

006	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	APPLICATION LAYER PROTOCOL: WEB PROTOCOLS (T1071.001)	Gli avversari possono comunicare usando protocolli web per confondersi con il traffico normale ed evitare il filtraggio di rete.
007	COMMAND AND CONTROL (TA0011)	APPLICATION LAYER PROTOCOL (T1071)	APPLICATION LAYER PROTOCOL: WEB PROTOCOLS (T1071.001)	Gli avversari possono comunicare usando protocolli del livello applicativo associati al traffico web per evitare il rilevamento.
008	PRIVILEGE ESCALATION (TA0004)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Gli avversari possono creare o modificare processi di sistema per ottenere privilegi elevati ed eseguire payload malevoli.
009	EXECUTION (TA0002)	COMMAND AND SCRIPT INTERPRETER (T1059)	—	Gli avversari possono abusare di interpreti di comandi e script per eseguire comandi, script o binari.
010	PERSISTENCE (TA0003)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Gli avversari possono creare o modificare processi di sistema per mantenere la persistenza del malware tra i riavvii del sistema.
011	PERSISTENCE (TA0003)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Creazione o modifica di processi di sistema per garantire persistenza del payload malevolo.
012	EXECUTION (TA0002)	SHARED MODULES (T1129)	—	Gli avversari possono eseguire payload malevoli caricando moduli condivisi.

013	PERSISTENCE (TA0003)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Persistenza attraverso la modifica/creazione di processi di sistema.
014	IMPACT (TA0040)	DATA DESTRUCTION (T1485)	—	Gli avversari possono distruggere dati e file su sistemi specifici o su larga scala per interrompere la disponibilità di sistemi, servizi e risorse di rete.
015	EXECUTION (TA0002)	SHARED MODULES (T1129)	—	Esecuzione di payload tramite caricamento di moduli condivisi.
016	PERSISTENCE (TA0003)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Persistenza attraverso la creazione o modifica di processi di sistema.
017	EXECUTION (TA0002)	SHARED MODULES (T1129)	—	Esecuzione di payload tramite moduli condivisi.
018	EXECUTION (TA0002)	SCHEDULED TASK/JOB (T1053)	—	Gli avversari possono abusare delle funzionalità di scheduling per eseguire codice malevolo in modo ricorrente o iniziale.
019	IMPACT (TA0040)	DATA DESTRUCTION (T1485)	—	Gli avversari possono distruggere dati e file per causare indisponibilità di sistemi e risorse.
020	IMPACT (TA0040)	SERVICE STOP (T1489)	—	Gli avversari possono fermare o disabilitare servizi di sistema per renderli indisponibili agli utenti legittimi.

021	IMPACT (TA0040)	DATA DESTRUCTION (T1485)	—	Distruzione dati e file su sistemi specifici o su larga scala per interrompere la disponibilità di sistemi e risorse.
022	IMPACT (TA0040)	DATA DESTRUCTION (T1485)	—	Distruzione dati e file su sistemi specifici o su larga scala per interrompere la disponibilità di sistemi e risorse.
023	PRIVILEGE ESCALATION (TA0004)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Creazione o modifica di processi di sistema per ottenere privilegi elevati ed eseguire payload malevoli.
024	DEFENSE EVASION (TA0005)	MASQUERADING (T1036)	—	Gli avversari possono manipolare le caratteristiche degli artefatti per farli apparire legittimi o benigni a utenti e strumenti di sicurezza.
025	PRIVILEGE ESCALATION (TA0004)	CREATE OR MODIFY SYSTEM PROCESS (T1543)	—	Creazione o modifica di processi di sistema per ottenere privilegi elevati.
026	IMPACT (TA0040)	SERVICE STOP (T1489)	—	Gli avversari possono fermare o disabilitare servizi di sistema per renderli indisponibili agli utenti legittimi.
027	IMPACT (TA0040)	MANIPULATION OF CONTROL (T0833)	—	Manipolazione dei processi fisici industriali, modificando parametri, tag o valori per causare perdita di visibilità e confusione operativa.

028	INHIBIT RESPONSE FUNCTION (TA0107)	DENIAL OF SERVICE (T0814)	—	Gli avversari possono eseguire attacchi DoS per interrompere le funzionalità attese dei dispositivi industriali.

7.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti. Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
INDUSTROYER	S0604	Malware modulare progettato per colpire sistemi ICS, in particolare sottostazioni elettriche. Utilizzato nell'attacco alla rete elettrica ucraina del 2016, è noto anche come CRASHOVERRIDE.
INDUSTROYER2	S1072	Variante aggiornata di Industroyer scoperta nel 2022, focalizzata sull'utilizzo del protocollo IEC-104 per colpire sottostazioni ad alta tensione.
BLACKENERGY	S0089	Toolkit malware usato per attacchi DDoS, sabotaggio e accesso remoto ai sistemi. Impiegato nell'attacco alla rete elettrica ucraina del 2015; capace di persistence, credential access e command execution.
KILLDISK	S0448	Malware distruttivo utilizzato in congiunzione con BlackEnergy per cancellare dati e danneggiare i sistemi delle vittime. Finalizzato al sabotaggio e alla negazione del servizio (DoS permanente).

Table 41: Tool associati alla campagna CRASHOVERRIDE

7.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
SCADA/ICS Software	Applicazione industriale	Target principale degli attacchi Sandworm tramite moduli malevoli personalizzati (es. IEC-101, IEC-104, OPC). Vulnerabilità sfruttate per esecuzione comandi su sottostazioni elettriche.
Microsoft Windows	Sistema Operativo	Utilizzato come piattaforma di esecuzione del malware Industroyer/Industroyer2 e per l'installazione di KillDisk. Sfruttate vulnerabilità note per privilege escalation e persistenza.
Protocollo IEC-104	Protocollo industriale	Manipolato attivamente dal modulo `104.dll` per inviare comandi falsificati (es. apertura/chiusura interruttori), causando blackout nelle sottostazioni.
OPC Data Access	Middleware industriale	Colpito tramite moduli che abusano di interfacce COM per interrompere la comunicazione tra SCADA e dispositivi di campo. Nessuna vulnerabilità nota specifica, ma abuso della logica di protocollo.
Remote Management Services	Servizio di rete	Utilizzati per movimenti laterali e persistenza (es. PsExec, SMB, RDP). L'assenza di segmentazione di rete ha facilitato l'escalation da IT a OT.
Sistemi HMI (Human-Machine Interface)	Interfaccia operatore	Target secondario per causare confusione o blocchi operativi; in alcuni casi manipolati per falsificare lo stato di impianti elettrici.

Table 42: Prodotti e componenti vulnerabili nelle campagne Sandworm associate a CRASHOVERRIDE

7.6 IoC

Gli *Indicators of Compromise* (IoC) relativi alla campagna **CRASHOVERRIDE**, condotta dal gruppo APT **Sandworm**, sono riportati in dettaglio nel report tecnico pubblicato da *ESET* in collaborazione con *Dragos*. Tali indicatori includono hash SHA256 dei moduli malevoli (es. `104.dll`, `opc.dll`), indirizzi IP e domini associati all'infrastruttura C&C, nonché regole YARA per l'identificazione di file e comportamenti riconducibili al malware.

Per un'analisi completa e l'elenco degli IoC raccolti durante l'analisi della campagna, si rimanda alle pagine **28** e **29** del report ufficiale.

7.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, 'e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell'attacco:

Fase	**Tool suggerito**	**Note operative**
Accesso iniziale (phishing)	GoPhish	Simulazione di campagne spear-phishing per ottenere accesso iniziale tramite allegati o link malevoli.
Esecuzione codice su host ICS	Metasploit	Simulazione dell'iniezione di payload in ambienti simulati o VM ICS (es. con moduli crafted simili a 104.dll).
Movimento laterale	CrackMapExec	Simulazione di movimenti laterali tramite SMB, WMI e autenticazione su altri nodi ICS.
Interazione con protocolli ICS	Scapy	Emulazione di comandi IEC-104, DNP3 o IEC 61850 inviati da host compromessi a dispositivi simulati.
Impatto (sabotaggio ICS)	Custom script Python + Scapy	Invio di pacchetti ICS falsificati per disabilitare o modificare lo stato di breaker simulati (interruttori).
Persistenza e accesso remoto	Metasploit persistence	Configurazione di backdoor persistenti e tunneling per accesso remoto anche dopo reboot.
C2 e controllo remoto	Metasploit	Comando e controllo centralizzato di più agenti, incluso supporto a moduli custom su target ICS.
Logging e osservabilità attacco	Wireshark	Analisi del traffico ICS malevolo e logging delle operazioni per valutazione forense.

Table 43: Tool consigliati per la simulazione in ambiente controllato

8 Extra: Ransomware Conti

Introduzione

Nel mondo della **cybersecurity**, pochi eventi hanno fatto tanto rumore quanto il caso

ContiLeaks. Fino al 2022, il gruppo **ransomware Conti** era uno dei più temuti e attivi al mondo: colpiva **aziende**, ospedali e istituzioni pubbliche, criptando i dati e chiedendo riscatti milionari. Si trattava di un vero e proprio "business criminale" gestito in modo quasi aziendale, con gerarchie, stipendi e persino bonus per i **cybercriminali** più produttivi.

Tutto cambia nel febbraio 2022, quando scoppia la guerra tra **Russia** e **Ucraina**. Il gruppo Conti si schiera apertamente a favore della **Russia**, pubblicando un comunicato che promette ritorsioni contro chiunque attacchi il governo russo. Questa presa di posizione causa una spaccatura interna: alcuni membri, probabilmente di origine **ucraina**, si sentono traditi e decidono di reagire.

È così che nasce **ContiLeaks**: uno o più membri interni cominciano a pubblicare online migliaia di **chat interne** del gruppo, **manuali di istruzioni**, liste di vittime, strumenti e persino il **codice sorgente** del ransomware. Per la prima volta, il mondo della **sicurezza informatica** può vedere da vicino come lavora una gang di ransomware: dai piani per attaccare grandi aziende ai trucchi per non farsi scoprire, passando per discussioni quotidiane, litigi interni e dettagli su come si spartiscono i soldi dei riscatti.

Questo **leak** ha rappresentato un vero colpo di scena: le informazioni rese pubbliche hanno permesso alle aziende di difendersi meglio, agli esperti di sicurezza di migliorare le strategie di prevenzione e alle **forze dell'ordine** di identificare alcuni membri del gruppo. Alla fine, tutta questa esposizione ha contribuito a indebolire e disgregare il gruppo Conti, che da allora non è più stato lo stesso.

ContiLeaks è così diventato uno degli esempi più clamorosi di come la **criminalità informatica** possa essere "ferita dall'interno", e di come la collaborazione, anche involontaria, tra nemici possa cambiare le regole del gioco nella **cybersicurezza**.

8.1 ContiLeaks

Il report **"Analysis of Conti Leaks"** analizza una delle più importanti **fughe di dati** della cybercriminalità recente, relativa al gruppo ransomware **Conti**. Il documento si basa sull'analisi di **chat interne**, **strumenti** e **tutorial** usati dal gruppo, resi pubblici tramite l'account Twitter "ContiLeaks" da **febbraio 2022**.

Il report descrive in dettaglio l'**organizzazione interna** del gruppo Conti, la **divisione dei ruoli** tra i membri e le loro modalità operative, simili a quelle di una vera e propria

startup tecnologica. Vengono illustrate le principali **tecniche di attacco**, come lo sfruttamento di dispositivi **IoT**, servizi **RDP** e **Domain Controller Windows**. Sono inoltre analizzati strumenti come **TrickBot**, **CobaltStrike**, **Emotet** e altri **tool interni** per la gestione dei botnet e delle vittime.

La parte sulle **vittime** mostra che Conti ha preso di mira **organizzazioni di ogni dimensione**, soprattutto nei settori **servizi** e **manifatturiero**, con particolare incidenza su aziende **statunitensi**. Il report sottolinea anche l'uso massiccio di **phishing**, **social engineering**, l'acquisto o lo sviluppo di **exploit** e la negoziazione di accessi tramite **broker** specializzati.

Infine, vengono analizzati due **tutorial interni**: uno rivolto agli "**hacker**" e uno ai "**ricercatori**", che forniscono consigli su come penetrare nelle reti delle vittime, eludere i sistemi di difesa e consolidare la presenza all'interno dei sistemi compromessi.

L'analisi offre quindi una panoramica completa su come agiscono le **organizzazioni ransomware** moderne, sia dal punto di vista **tecnico** che **gestionale**, e suggerisce spunti utili per la **difesa delle reti aziendali** da queste minacce.

8.2 Analisi Vulnerabilità

Nel corso dell'analisi di questo report sono state identificate le seguenti vulnerabilita':

Campo	Valore
cve	CVE-2020-5135
cvss-bt_score	9.8
cvss-bt_severity	CRITICAL
cvss-bt_vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H
cvss_version	3.1
base_score	9.8
base_severity	CRITICAL
base_vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
assigner	PSIRT@sonicwall.com
published_date	2020-10-12T11:15Z
epss	0.35654
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	False
nuclei	False
poc_github	False
cwe	CWE-120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow)
cpe	SonicWall SonicOS 6.5.4.7-79n e precedenti

La vulnerabilità **CVE-2020-5135** interessa **SonicWall SonicOS** (versione **6.5.4.7-79n** e precedenti) e permette attacchi di tipo **buffer overflow**, con rischio **critico** (**CVSS 9.8**). È riconosciuta nei principali **database di sicurezza**, ma al momento non risultano **exploit pubblici** o moduli **Metasploit** disponibili.

Le informazioni temporali sui CVE relative a **ContiLeaks** sono le seguenti:

Punto	Dettaglio
Tipo	Vulnerabilità di esecuzione di codice remoto su dispositivi SonicWall (SonicOS), sfruttabile via pacchetti UDP appositamente creati (stack overflow).
Divulgazione	Divulgata pubblicamente il 14 ottobre 2020, da Secura, con advisory e PoC pubblici.
Zero day?	Non utilizzata come zero-day nei casi noti: patch e dettagli erano già pubblici prima dello sfruttamento da parte di Conti.
Patch	SonicWall ha rilasciato patch e mitigazioni ufficiali dal 13 ottobre 2020 per tutte le versioni vulnerabili di SonicOS.
Utilizzo nel malware	Discussioni nei leak mostrano che Conti valutava attivamente l'acquisto e la ricerca di exploit per SonicWall. Gli exploit per CVE-2020-5135 sono stati utilizzati per ottenere accesso iniziale su target non aggiornati.

Table 44: Informazioni temporali per CVE-2020-5135 (ContiLeaks)

8.3 TTP MITRE ATT&CK

Le TTP che abbiamo rilevato sono le seguenti :

ID	Tactic	Technique	Sub-technique	Descrizione
001	IMPACT (TA0040)	DATA LEAK (T1565.002)	Data Leaked (T1565.002)	Diffusione pubblica di dati violati e pubblica umiliazione delle vittime per aumentare la pressione e ottenere il pagamento del riscatto dalle organizzazioni colpite.
002	RECONNAISSANCE (TA0043)	SEARCH VICTIM-OWNED DEVICES (T1595)	RESEARCH VULNERABILITIES (T1595.002)	Acquisto e analisi di router/firewall Sonicwall e Cisco per individuare e sviluppare exploit su vulnerabilità note, come CVE-2020-5135.

003	INITIAL ACCESS (TA0001)	PHISHING (T1566)	—	I membri di Conti si affidano fortemente a campagne di spam e phishing, spesso utilizzando software specializzato per automatizzare e gestire operazioni di phishing su larga scala nella fase di accesso iniziale.
004	DEFENSE EVASION (TA0005)	OBFUSCATED FILES OR INFORMATION (T1027)	—	Il gruppo lavora costantemente per eludere gli antivirus, sviluppando e utilizzando tecniche per aggirare o disabilitare i software di sicurezza e sfuggire al rilevamento.
005	INITIAL ACCESS (TA0001) / COLLECTION (TA0009)	VALID ACCOUNTS (T1078) / EMAIL COLLECTION (T1114)	—	Il gruppo ha ottenuto accesso non autorizzato a uno o più account email di individui specifici, probabilmente per raccogliere informazioni sensibili o facilitare ulteriori compromissioni.
005	INITIAL ACCESS (TA0001)	VALID ACCOUNTS (T1078)	—	I membri del gruppo negoziano con broker di accesso per ottenere accessi non autorizzati agli ambienti delle vittime, spesso acquistando credenziali o altri metodi di accesso.
005	INITIAL ACCESS (TA0001)	VALID ACCOUNTS (T1078)	—	I membri del gruppo discutono di avere un insider all'interno di alcune banche indiane per facilitare l'accesso non autorizzato a sistemi o dati interni.

006	INITIAL ACCESS (TA0001)	SEARCH VICTIM-OWNED DEVICES (T1595)	—	I dispositivi IoT sono considerati un'importante superficie di attacco iniziale, spesso presi di mira per la loro esposizione, configurazioni di sicurezza deboli e vulnerabilità, fornendo un possibile punto di ingresso nelle reti bersaglio.
007	INITIAL ACCESS (TA0001)	EXTERNAL REMOTE SERVICES (T1133)	—	L'RDP (Remote Desktop Protocol) è raccomandato come backdoor iniziale, consentendo agli attaccanti di stabilire accesso remoto e mantenere la persistenza sfruttando servizi remoti esposti o compromessi nelle reti delle vittime.
008	PERSISTENCE (TA0003)	MANIPULATION (T1098)	—	I server Active Directory sono spesso l'obiettivo principale degli attaccanti prima di stabilire la persistenza, poiché comprometterli permette movimento laterale esteso e controllo persistente sull'ambiente della vittima.

009	INITIAL ACCESS (TA0001)	EXPLOIT PUBLIC-FACING APPLICATION (T1190)	—	Qualsiasi servizio di rete pubblico, come un indirizzo IP pubblico con una porta aperta, è considerato un potenziale punto di ingresso per gli attaccanti che sfruttano vulnerabilità o errori di configurazione per ottenere accesso iniziale.
010	INITIAL ACCESS (TA0001), PERSISTENCE (TA0003)	EXTERNAL REMOTE SERVICES (T1133)	—	Servizi legittimi come VPN, thin client, RDWeb e RDP esposti a Internet possono essere sfruttati dagli attaccanti per creare una "backdoor ideale", consentendo accesso remoto persistente e spesso poco rilevabile nell'ambiente della vittima.
011	CREDENTIAL ACCESS (TA0006)	CREDENTIAL DUMPING (T1003)	—	Gli attaccanti cercano credenziali e computer accessibili all'interno della rete bersaglio per ottenere accesso ai servizi. L'uso di password deboli o riutilizzate facilita la compromissione tramite raccolta credenziali, forza bruta o uso di account validi rubati.

012	LATERAL MOVEMENT (TA0008)	REMOTE SERVICES (T1021), LATERAL TOOL TRANSFER (T1570)	—	L'accesso a nodi critici come Active Directory permette agli attaccanti di eseguire movimento laterale esteso, usando servizi remoti e trasferimento di strumenti per spostarsi tra i sistemi ed elevare i privilegi.
013	RECONNAISSANCE (TA0043)	GATHER VICTIM IDENTITY INFORMATION (T1589)	GATHER VICTIM ORGANIZATION INFORMATION (T1589.002)	Alcuni tutorial includono istruzioni su come raccogliere informazioni utili su persone e organizzazioni tramite piattaforme social come LinkedIn, per preparare e personalizzare ulteriori fasi dell'attacco.

8.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti.Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
BazarLoader	S0534	Loader modulare utilizzato per il caricamento di payload dannosi e per fornire accesso iniziale alle reti delle vittime; spesso usato come punto di ingresso per ransomware.
TrickBot	S0266	Malware bancario evoluto in una piattaforma modulare, usato per il furto di credenziali, la diffusione laterale in rete e l'installazione di altri malware come ransomware.

Tool	ID MITRE	Descrizione
Cobalt Strike	S0154	Framework legittimo per il penetration testing spesso abusato dagli attaccanti per il comando e controllo, la movimentazione laterale e il rilascio di payload su sistemi compromessi.
Emotet	S0367	Malware modulare inizialmente nato come trojan bancario, ora usato principalmente come dropper per altri malware e ransomware all'interno delle reti compromesse.

Table 46: Tool principali associati al framework MITRE ATT&CK.

8.5 Informazioni sui prodotti vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
Microsoft Windows	Sistema Operativo	Vulnerabilità di Active Directory e Domain Controller sfruttate tramite exploit noti (es. Zerologon), misconfigurazioni comuni e servizi esposti (come RDP e VPN) che possono essere abusati per accesso iniziale e movimento laterale nella rete.
SonicWall Firewall	Dispositivo di rete	Vulnerabilità come CVE-2020-5135 sfruttata tramite analisi diretta e sviluppo di exploit ad hoc, facilitando accesso iniziale o persistenza nella rete aziendale.
Cisco Router/Firewall	Dispositivo di rete	Dispositivi spesso target di ricerca e sviluppo exploit, specialmente se esposti su Internet, consentendo agli attaccanti di ottenere l'accesso iniziale alle reti aziendali.
Dispositivi IoT/OT (stampanti, PLC, smart firewall, router)	Dispositivo integrato	Frequentemente esposti e raramente aggiornati, con configurazioni di sicurezza deboli e vulnerabilità note, rappresentano un punto di ingresso privilegiato per l'attaccante.
WordPress e altri CMS	Applicazione Web	Possibile sfruttamento di vulnerabilità nei plugin o nel core dell'applicazione per ottenere accesso iniziale alle infrastrutture aziendali.
VPN, RDWeb, Thin Client	Servizi remoti	Servizi legittimi esposti pubblicamente possono essere sfruttati dagli attaccanti per ottenere persistenza e accesso continuativo, soprattutto in presenza di credenziali deboli o riutilizzate.

Table 47: Prodotti e superfici di attacco tipicamente sfruttati nelle campagne Conti

8.6 IoC

Gli **Indicators of Compromise** (**IoC**) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del **report originale**, all'interno dell'**appendice**. In questa sezione finale del **PDF** (pag 14) è possibile trovare esempi di **hash**, **nomi di file**, **URL** malevoli, **domini** di **command and control**, **percorsi di debug** e altri indicatori tecnici associati alle varie famiglie di **malware** descritte nel rapporto.

8.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, 'e possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi dell'attacco:

Fase	Tool suggerito	Note operative
Ricognizione iniziale	Recon-ng, theHarvester, SpiderFoot	Raccolta informazioni su domini, indirizzi email, e infrastruttura pubblica dell'organizzazione target.
Raccolta informazioni sugli utenti	LinkedIn, Sherlock, holehe	Ricerca di account social e username correlati agli utenti target tramite OSINT.
Simulazione phishing	GoPhish	Invio di email di phishing con allegati o link malevoli e monitoraggio delle aperture/click, in modo controllato.
Generazione payload e allegati malevoli	Metasploit Framework	Creazione di file Word/PDF con macro o exploit per la simulazione dell'accesso remoto iniziale.
Accesso remoto e post-exploitation	Metasploit Framework, Covenant, Powershell Empire	Gestione delle sessioni post-exploitation, raccolta credenziali e movimento laterale simulato.
Simulazione movimento laterale	Impacket, CrackMapExec	Esecuzione di comandi da remoto, raccolta e utilizzo di credenziali, simulazione di attacchi "living off the land".
Esfiltrazione dati simulata	RClone, Ncat, rsync	Simulazione di trasferimento file da host compromessi verso server di test o storage cloud controllati dall'audit team.

Table 48: Fasi e tool open source per simulare una campagna Conti in modo legale

9 Extra: Ransomware BlackBasta

Introduzione

Black Basta è un **ransomware** emerso per la prima volta intorno ad **aprile 2022** e rapidamente diventato uno dei gruppi più attivi nella scena del **cybercrime**. Si tratta di un **ransomware as-a-service (RaaS)**, ovvero una piattaforma utilizzata da diversi

affiliati per condurre attacchi contro aziende e organizzazioni in tutto il mondo, in particolare nei settori **manifatturiero**, **sanitario**, **servizi** e **infrastrutture critiche**. **Black Basta** cifra i dati delle vittime, rendendoli inaccessibili, e contemporaneamente adotta la **doppia estorsione**: non solo richiede un **riscatto** per decriptare i file, ma minaccia anche di **pubblicare dati sensibili** rubati su un proprio sito dedicato (`Basta News`) nel **dark web**, per aumentare la pressione sulle vittime. Questo gruppo si distingue per l'utilizzo di **tecniche di attacco avanzate**, l'impiego di strumenti di **living-off-the-land** (cioè tool già presenti nei sistemi compromessi) e la capacità di colpire sia ambienti **Windows** sia **server VMware ESXi**. Le campagne di **Black Basta** sfruttano spesso l'accesso iniziale tramite **phishing**, **exploit di vulnerabilità note**, o **acquisto di credenziali rubate**, e includono una rapida **escalation dei privilegi** e **movimento laterale** nella rete. Una volta completata la fase di **esfiltrazione dei dati**, viene avviata la **cifratura**. In breve, **Black Basta** rappresenta oggi una delle principali **minacce ransomware** a livello globale, nota per la **velocità d'azione**, l'efficacia delle proprie tecniche di **estorsione** e la capacità di adattarsi a diversi **target** e **infrastrutture IT**.

9.1 Ransomware Roundup - Black Basta

Il report di FortiGuard Labs su **Black Basta** fornisce una panoramica aggiornata su questo ransomware, attivo dal 2022 e considerato tra i principali gruppi della scena. Black Basta prende di mira sia sistemi Windows sia server VMWare ESXi, colpendo aziende di vari settori, soprattutto in Europa e Nord America. Il gruppo adotta un modello *Ransomware-as-a-Service* (RaaS): mette a disposizione infrastruttura e malware a degli affiliati, che scelgono le vittime, rubano dati e avviano la cifratura dei file. Se il riscatto non viene pagato, i dati sottratti vengono pubblicati online (doppia estorsione). Per ottenere l'accesso iniziale, Black Basta sfrutta e-mail di spear-phishing, acquisto di credenziali tramite broker, e l'uso di malware come QakBot (QBot). Utilizza anche exploit noti come PrintNightmare (CVE-2021-34527) e Follina (CVE-2022-30190). Una volta entrati nella rete, gli affiliati usano strumenti come PsExec, PowerShell, Mimikatz, CobaltStrike, Netcat e altri per muoversi lateralmente e rubare dati (ad esempio con RClone) prima della cifratura. Il ransomware impiega algoritmi avanzati di cifratura (`XChaCha20`) e genera estensioni di file cifrati personalizzate. Su Windows è distribuito come eseguibile o DLL; su Linux/ESXi esiste una variante mirata ai file delle macchine

virtuali. La richiesta di riscatto viene presentata tramite un file di testo che istruisce la vittima a collegarsi a un sito Tor per la negoziazione. Il gruppo gestisce anche un sito "name and shame" su Tor dove pubblica i dati delle vittime che non pagano. Secondo i dati Fortinet, oltre il 60% delle vittime sono aziende statunitensi, ma sono colpiti anche Germania, Canada, Italia, UK e Slovenia. I settori più colpiti sono manifatturiero, costruzioni, servizi e retail. La maggior parte delle vittime ha subito la pubblicazione totale o parziale dei dati. Il report ricorda che le soluzioni Fortinet permettono di rilevare e bloccare Black Basta con firme antivirus e protezioni EDR. Viene sottolineata l'importanza di mantenere aggiornati antivirus e sistemi di rilevamento, oltre a implementare strategie di backup e segmentazione della rete per contenere i danni di attacchi simili.

9.2 Analisi Vulnerabilità

Nel corso dell'analisi di questo report sono state identificate le seguenti vulnerabilità:

Campo	Valore
cve	CVE-2021-34527
cvss-bt_score	9.0
cvss-bt_severity	HIGH
cvss-bt_vector	AV:N/AC:L/Au:S/C:C/I:C/A:C/E:H
cvss_version	2.0
base_score	9.0
base_severity	HIGH
base_vector	AV:N/AC:L/Au:S/C:C/I:C/A:C
assigner	secure@microsoft.com
published_date	2021-07-02T22:15Z
epss	0.94257
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Windows 7/8.1/10/11. Windows Server 2008/2012/2016/2019/2022

La tabella riporta una sintesi dettagliata delle principali informazioni relative alla vulnerabilità **CVE-2021-34527**, conosciuta anche come **PrintNightmare**. Vengono elencati tutti i parametri chiave per la valutazione del rischio, come il punteggio **CVSS** (**9.0**, severità **HIGH**), il vettore di attacco, la versione del sistema di scoring, e la presenza di exploit pubblici su vari framework (come **Metasploit** e **GitHub**). Sono indicati anche dettagli operativi come l'**assigner** della vulnerabilità, la **data di pubblicazione**, l'indice **EPSS** e la presenza nella lista **CISA KEV**. La voce **CWE** indica che, per questa

vulnerabilità, nelle fonti ufficiali non è disponibile una classificazione tecnica dettagliata, mentre la **CPE** fornisce un elenco compatto ma esplicativo dei **sistemi operativi Microsoft Windows** interessati, includendo tutte le versioni principali di client e server coinvolte nel 2021. La tabella permette di avere a colpo d'occhio sia la **valutazione del rischio** che la **rilevanza operativa** della vulnerabilità.

Campo	**Valore**
cve	CVE-2022-30190
cvss-bt_score	9.3
cvss-bt_severity	HIGH
cvss-bt_vector	AV:N/AC:M/Au:N/C:C/I:C/A:C/E:H
cvss_version	2.0
base_score	9.3
base_severity	HIGH
base_vector	AV:N/AC:M/Au:N/C:C/I:C/A:C
assigner	secure@microsoft.com
published_date	2022-06-01T20:15Z
epss	0.93384
cisa_kev	True
vulncheck_kev	True
exploitdb	False
metasploit	True
nuclei	False
poc_github	True
cwe	NVD-CWE-noinfo: Insufficient Information
cpe	Microsoft Windows MSDT (Microsoft Support Diagnostic Tool), v7,v8.1,v10,v11. Windows Server 2008/2012/2016/2019/2022

Questa tabella presenta una **sintesi dettagliata** delle principali informazioni riguardanti la vulnerabilità **CVE-2022-30190**, conosciuta anche come "**Follina**". Vengono riportati i valori di **gravità** secondo il sistema **CVSS**, il **vettore di attacco** e le informazioni di base come l'**assegnazione**, la **data di pubblicazione** e il punteggio **EPSS** che indica la probabilità di sfruttamento. Sono indicati anche i **database** e gli **strumenti** in cui la vulnerabilità è presente, come **Metasploit** e **GitHub**, nonché l'inclusione nei cataloghi **CISA** e **Vulncheck**. Il campo **CWE** indica che la classificazione specifica della vulnerabilità non è stata dettagliata ("**Insufficient Information**"), mentre il campo **CPE** riassume chiaramente i prodotti affetti, ovvero varie versioni di **Microsoft Windows MSDT** e i principali sistemi **Windows Server**. In questo modo, la tabella offre una **panoramica immediata** e **completa** per comprendere la **pericolosità**, la **diffusione** e i **target** della vulnerabilità.

Le informazioni temporali relative alle CVE contenute nel report analizzato per **Blackbasta** sono le seguenti:

Punto	**Dettaglio**
Tipo	Vulnerabilità di esecuzione di codice remoto tramite Microsoft Support Diagnostic Tool (MSDT) sfruttando documenti Office malevoli (Word, RTF) per lanciare comandi sul sistema vittima.
Divulgazione	Pubblicata a fine maggio 2022, con exploit e PoC subito disponibili in rete e rapidamente sfruttati in campagne reali.
Zero day?	Al momento della scoperta era zero-day; durante le principali campagne Black Basta, era già nota e sfruttata in modo massivo su sistemi non aggiornati.
Patch	Patch ufficiale rilasciata da Microsoft il 14 giugno 2022 (Patch Tuesday).
Utilizzo nel malware	Utilizzata in attacchi mirati tramite allegati Word/RTF veicolati con phishing, spesso per ottenere l'accesso iniziale alla rete da parte di affiliati Black Basta.

Table 49: Dettagli temporali per CVE-2022-30190 (Follina)

Punto	Dettaglio
Tipo	Vulnerabilità di escalation dei privilegi tramite Print Spooler di Windows ("PrintNightmare"), che permette esecuzione di codice remoto.
Divulgazione	Divulgata pubblicamente a giugno 2021, con exploit disponibili su GitHub nel giro di pochi giorni.
Zero day?	Sfruttata come zero-day poco dopo la pubblicazione; successivamente il malware colpiva soprattutto sistemi non patchati.
Patch	Patch ufficiale pubblicata da Microsoft a luglio 2021.
Utilizzo nel malware	Sfruttata per movimento laterale ed escalation di privilegi durante attacchi ransomware come Black Basta, spesso come parte di catene di exploit più articolate.

Table 50: Dettagli temporali per CVE-2021-34527 (PrintNightmare)

9.3 TTP MITRE ATT&CK

Le TTP che abbiamo rilevato sono le seguenti:

ID	Tactic	Technique	Sub-technique	Descrizione
001	IMPACT (TA0040)	DATA ENCRYPTION FOR IMPACT (T1486)	—	Gli attaccanti possono cifrare dati su sistemi target o su molti sistemi in rete per interrompere la disponibilità delle risorse, chiedendo poi un riscatto per decriptare i file e ripristinare l'accesso.

002	IMPACT (TA0040)	INHIBIT SYSTEM RECOVERY (T1490)	—	Gli avversari possono creare e gestire infrastrutture come portali di pagamento per facilitare il pagamento del riscatto e il ripristino delle operazioni da parte delle vittime.
003	LATERAL MOVEMENT (TA0008)	LATERAL TOOL TRANSFER (T1570)	—	Gli attaccanti possono spostarsi lateralmente nella rete trasferendo strumenti o malware tra i sistemi per ottenere l'accesso ad altri asset o dati sensibili.
004	DEFENSE EVASION (TA0005)	SIGNED BINARY PROXY EXECUTION (T1218)	—	Gli attaccanti possono abusare di binari di sistema legittimi e firmati (LOLbins) già presenti nel sistema per svolgere azioni malevole ed eludere i controlli di sicurezza.
005	COLLECTION (TA0009)	DATA STAGED (T1074)	—	Gli avversari possono cercare e raccogliere file sensibili, aggregando i dati prima di esfiltrarli come parte della doppia estorsione.
006	EXFILTRATION (TA0010)	EXFILTRATION OVER WEB SERVICE (T1567)	—	Gli attaccanti possono trasferire i dati raccolti a infrastrutture remote tramite web services, cloud storage o altri canali nascosti.

007	INITIAL ACCESS (TA0001)	PHISHING (T1566)	SPEARPHISHING LINK (T1566.002)	Gli avversari possono inviare email mirate con link o allegati malevoli, cercando di ingannare il destinatario per ottenere l'accesso iniziale all'ambiente della vittima.
008	DEFENSE EVASION (TA0005)	OBFUSCATED FILES OR INFORMATION (T1027)	—	Gli attaccanti possono personalizzare il ransomware per ciascuna vittima, ad esempio inserendo un Login ID unico o estensioni di file custom, rendendo l'attacco più difficile da rilevare e facilitando la negoziazione.
009	IMPACT (TA0040)	Extortion (T1657)	—	Dopo la cifratura dei file e la pubblicazione della nota di riscatto, la vittima viene istruita a contattare il gruppo tramite servizi nascosti Tor, garantendo anonimato agli attaccanti.
010	IMPACT (TA0040)	DATA ENCRYPTION FOR IMPACT (T1486)	—	Il ransomware può essere programmato per aprire automaticamente la nota di riscatto dopo la cifratura, aumentando la probabilità che la vittima la legga subito.

012	EXECUTION (TA0002)	COMMAND AND SCRIPTING INTERPRETER (T1059)	—	L'uso di flag specifici da linea di comando indica che il ransomware è pensato per essere eseguito manualmente su server ESXi compromessi, consentendo all'attaccante di controllarne il comportamento.
013	IMPACT (TA0040)	DATA ENCRYPTION FOR IMPACT (T1486)	T1589.002: Publish Data	Gli attaccanti possono gestire un sito di "name and shame" sulla rete Tor, esponendo nomi e dati delle vittime che non pagano il riscatto, aumentando la pressione tramite danno reputazionale e minaccia di pubblicazione.

9.4 Tool Utilizzati

Nella campagna d'attacco analizzata sono stati trovati alcuni strumenti utilizzati da parte degli attaccanti. Di seguito sono riportati gli strumenti:

Tool	**ID MITRE**	**Descrizione**
PsExec	S0029	Strumento Microsoft per esecuzione di processi su sistemi remoti tramite autenticazione; comunemente utilizzato dagli attaccanti per movimento laterale e distribuzione di payload in reti Windows.

Tool	**ID MITRE**	**Descrizione**
QakBot	S0650	QakBot è frequentemente utilizzato come vettore iniziale per distribuire ransomware come Black Basta. Dopo l'infezione iniziale, QakBot consente agli attaccanti di ottenere accesso remoto, muoversi lateralmente nella rete e scaricare ulteriori payload, tra cui il ransomware Black Basta.
Windows Management Instrumentation (WMI)	S0197	Framework di gestione di sistemi Windows che consente esecuzione di comandi e script remoti; sfruttato per movimento laterale, raccolta informazioni e persistence sfruttando funzionalità native del sistema.
PowerShell	S0194	Shell e linguaggio di scripting di Windows; utilizzato dagli attaccanti per esecuzione di comandi, download e lancio di payload, evasione dei controlli, automazione delle attività malevole.
Netcat	S0039	Strumento di rete multipiattaforma per trasferimento dati, creazione di shell remote e tunneling di connessioni; impiegato per esfiltrazione dati, C&C e movimento laterale.
BITSAdmin	S0190	Utility Microsoft che gestisce trasferimenti di file in background; abusato per scaricare payload malevoli in modo stealth, eludendo sistemi di detection tradizionali.

Tool	**ID MITRE**	**Descrizione**
BCDEdit	—	Utility Windows per la modifica delle impostazioni di avvio del sistema operativo; può essere utilizzato per disabilitare meccanismi di protezione e facilitare la persistenza del malware.
SystemBC	S1033	Proxy backdoor modulare che consente routing del traffico C&C e download di payload, mascherando le comunicazioni malevole e favorendo l'evasione delle difese.
Mimikatz	S0002	Tool per l'estrazione di credenziali e hash dalle memorie di sistema Windows; ampiamente usato per privilege escalation e raccolta di credenziali in attacchi post-exploitation.
Cobalt Strike	S0154	Framework commerciale di red teaming usato da attori malevoli per comando e controllo, movimento laterale, esfiltrazione e deployment di beacon per il controllo remoto delle macchine compromesse.
Brute Ratel C4	S1063	Strumento avanzato di red teaming per esecuzione di payload, persistence, movimento laterale e comando e controllo, simile a Cobalt Strike ma meno rilevato da molte difese.

Tool	ID MITRE	Descrizione
Remote access tools	—	Suite di strumenti per accesso remoto e controllo dei sistemi target, spesso utilizzati per mantenere il controllo sulle reti compromesse.
RClone	S1040	Software open source di sincronizzazione e trasferimento file verso cloud storage; abusato per esfiltrare grandi volumi di dati dalle reti delle vittime.
Tor	S0183	Rete di anonimizzazione utilizzata per nascondere le comunicazioni C&C, pubblicare siti di pagamento e garantire privacy e irreperibilità agli attaccanti durante negoziazione e doppia estorsione.

9.5 Informazioni sui Prodotti Vulnerabili

Riportiamo alcuni dei prodotti, servizi e strumenti che sono stati sfruttati in questa campagna:

Prodotto	Tipologia	Note sulla vulnerabilità
Microsoft Windows	Sistema Operativo	Target principale delle campagne Black Basta; vulnerabilità sfruttate includono esecuzione di codice remoto (es. CVE-2022-30190 "Follina", CVE-2021-34527 "PrintNightmare"), privilege escalation e abuso di strumenti nativi come PowerShell, WMI e PsExec per movimento laterale e persistence.

Prodotto	**Tipologia**	**Note sulla vulnerabilità**
VMware ESXi	Hypervisor	Target di variante Linux del ransomware; vulnerabilità sfruttate riguardano l'accesso remoto e la cifratura dei volumi virtuali, con focus sui file delle VM (`.vmdk`, `.vmx`, `.vmsd`, `.vmxf`).
Microsoft Office	Applicazione	Utilizzata come vettore iniziale tramite spear-phishing con allegati Word o RTF contenenti macro o exploit (inclusi quelli per Follina, CVE-2022-30190).
Microsoft Support Diagnostic Tool (MSDT)	Strumento di sistema	Sfruttato tramite vulnerabilità "Follina" (CVE-2022-30190), che consente esecuzione di comandi arbitrari su sistemi Windows tramite documenti Office malevoli.
Windows Print Spooler	Servizio di sistema	Vulnerabilità PrintNightmare (CVE-2021-34527) sfruttata per escalation di privilegi e movimento laterale su sistemi Windows.

9.6 IoC

Gli *Indicators of Compromise* (IoC) analizzati e discussi all'interno di questo documento sono riportati in dettaglio nelle ultime pagine del report originale (da pag. 20 a 26). In questa sezione finale del PDF è possibile trovare esempi di hash e altri indicatori tecnici associati al ransomware BlackBasta descritto nel rapporto.

9.7 Elementi Utili alla Simulazione

Per simulare la campagna di attacco analizzata, è possibile pensare di sfruttare alcuni strumenti open source o framework commerciali, utili a riprodurre delle specifiche fasi

dell'attacco:

Fase	**Tool suggerito**	**Note operative**
Simulazione spear-phishing	GoPhish	Invio di email mirate con allegati o link malevoli (Word, RTF) per ottenere accesso iniziale su target di laboratorio.
Generazione e weaponizzazione di documenti	Metasploit, Python (exploit Follina)	Creazione di documenti Office o RTF contenenti macro, exploit (es. CVE-2022-30190 "Follina") o payload per apertura reverse shell.
Esecuzione di payload e movimento laterale	PsExec, PowerShell	Spostamento laterale sfruttando strumenti integrati Windows e trasmissione di malware su host aggiuntivi simulando le tecniche living-off-the-land.
Privilege escalation	Metasploit (exploit), Mimikatz	Sfruttamento di exploit per privilege escalation (es. PrintNightmare), estrazione di credenziali e hash tramite Mimikatz.
Persistenza	Metasploit persistence	Installazione di backdoor o beacon persistenti per mantenere il controllo sulle macchine compromesse.
Comando e controllo (C2)	Metasploit multi-handler	Gestione delle sessioni C2, invio comandi remoti, upload/download file tra vittima e attaccante.
Esfiltrazione dati	RClone, Python	Esportazione di dati simulati su server esterni o servizi cloud per riprodurre la fase di esfiltrazione (double extortion).
Simulazione infrastruttura Tor	Tor Browser, OnionShare	Simulazione della comunicazione via .onion e pubblicazione di file/ransom note su servizi Tor, come nel modello double extortion.