



#### NOTE DE SECURITE

|                            |                   |
|----------------------------|-------------------|
| <b>Titre</b>               | Malware “ Ramnit” |
| <b>Numéro de Référence</b> | 60352701/26       |
| <b>Date de Publication</b> | 27 Janvier 2026   |
| <b>Risque</b>              | Critique          |
| <b>Impact</b>              | Critique          |

Ramnit est un cheval de Troie bancaire sophistiqué, destiné principalement à voler les informations des comptes bancaires en ligne et les informations d'authentification saisies via les navigateurs web. Il cible principalement les systèmes Windows et se propage souvent via des campagnes phishing.

L'une des caractéristiques du logiciel malveillant Ramnit est l'utilisation d'un algorithme de génération de domaines (DGA) pour éviter les listes de blocage DNS lors de ces communications avec les serveurs de commande et contrôle (C2), rendant sa détection plus complexe. Le malware est capable d'infecter des fichiers EXE, DLL et HTML, assurant ainsi une persistance élevée et une propagation rapide au sein des systèmes compromis. Cependant, le logiciel malveillant Ramnit peut également déployer des modules supplémentaires pour installer autres logiciels malveillants.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT en cas de détection d'une activité relative à ce malware.

## Indicateurs de compromission (IOCs):

### Hashs :

- 7bc499fb39be1163ed141baa52f70003ead93cd9c0b13b45ff174eec59148187
- 0f5f6ee9958d6e1b89da082c1aeffd6a1f29ca59789ac6f448467e32bede7052
- 8baad520b274eeb0078ba9a4ee88b7fd7a4686d6551123f0200bd38f7b15e182
- 7da161aad78062af74fa0ad43b83bfa926ca52fb18c65ec5418675ad4ddf76c4
- 8545c5e6e85b07575dac153ec13c30b86023dad9a25107d42cc5d27bbdc449d8
- 7fa14e9444fb8d4f9af119a7fd76974e9b08d43028fea265415973cbfa9fc29a
- 5c722d7f47c4504d05fd3fb85cfc1a54951ff6db89daffa0cfe92d6b1c939b09
- 288d8f0b77bebc57dbf8dbfd704b7c9cc28b6d4ac7666f9df848743d8e5f6634
- 2b2322a2a02f5a9ab274637dd8a1875cb2256db12d9e044b38da6019fdbfa567
- 1264fb9a1706f3a239eea02adec3718c109a6de34dd1a38141e0352d47341795
- 141ff2b22db43166f130dad0deb69169e8f5a5632ea5dae8d972fafb486405d2
- 9ebf7cd2d5e49ca3b098453b156dbf9952f18e05c9707482dc1bc2c48d4824a0
- 3c39474bc6f50709e61b9bfdebd87ada96e41a9b1e0e8472ef7bd074cd632db1
- 23b843a53bd6dd4ea044acf4fed30a400d043ff7dd8fa2b9534f3d2cfe7e5321
- b6f09c818c177ec16ff52a271b6c789d7502fef40ee45a4980dfd932e6431f6e
- a038a20e4350d3fc4f4b117546749ea70fd05e7a6a090c3fc4ee13067430ea9f
- 5cb7b12de85124a09b9ef9d8988038b689d2649e450434ceecf653bf71bc8727
- 3abdd78ac954fa36156085c285a8810381fbf73e4924a353967a4df9f0ad8cc4
- d0463f872ec0070239be3399245e852971fadedf5b9fe1454c133241bc3b343a1
- 9738fd8e0dca3a194d7f5c48ddc0be1de5a71e384018b59b0d01c671afd0db17

### IP :

- |                 |                   |
|-----------------|-------------------|
| • 36.88.164.50  | • 36.88.136.42    |
| • 36.92.154.218 | • 36.95.104.66    |
| • 36.64.184.42  | • 36.92.154.194   |
| • 36.64.174.122 | • 36.92.154.234   |
| • 36.88.136.34  | • 36.88.164.154   |
| • 36.88.164.114 | • 36.89.252.226   |
| • 36.64.174.98  | • 36.92.154.178   |
| • 36.89.252.58  | • 36.88.164.130   |
| • 36.92.9.2     | • 36.64.174.170   |
| • 36.88.164.178 | • 113.161.113.211 |
| • 36.89.252.106 | • 36.89.252.242   |
| • 36.88.136.58  | • 189.44.91.12    |
| • 61.19.246.237 | • 36.89.252.26    |

- 47.104.227.108
- 36.92.154.34
- 36.64.174.154
- 36.64.174.210
- 36.95.104.130
- 36.92.154.106
- 47.104.139.94
- 36.88.164.194
- 36.64.184.26
- 36.89.252.178
- 36.88.136.194
- 36.64.175.50
- 36.95.104.242
- 36.92.154.42
- 36.88.164.170
- 36.88.164.138
- 101.42.139.46
- 106.53.218.253
- 36.64.174.194
- 36.88.164.210
- 36.88.164.218
- 36.64.184.50
- 36.89.252.82
- 27.17.46.66
- 139.129.95.12
- 36.64.174.114
- 121.61.112.86
- 103.148.232.117
- 36.92.154.2

#### Signature Malware :

- Win.Virus.Ramnit-9808983-0
- Virus.Win32.Nimnul.n!c
- Gene.Win.Harmlet.7967-0
- Trojan.Win32.DownLoad2.wtigj
- Suspicious:Trojan.Girtk.AE.uyht.mg
- Trojan.Zbot
- Win32.HLLW.Autoruner2.6551
- Gene.Win.Harmlet.3-3977
- Gene.Win.Harmlet.3-3705
- Trojan.Win32.Generic.ltev
- Virus.Win32.Nimnul
- Gene.Win.Harmlet.3-3900
- Gen.Heur
- Win.Malware.Ramnit-10015637-0
- Win32.Nimnul.1
- Win32/Virus.Ramnit.HygB8HkA
- Win32.HLLW.Facebook.2390
- Win32/Trojan.Dorv.HxQBepsA
- Virus.Win32.Ramnit
- Win32/Virus.Ramnit.HwsBrr0A

**N.B : La liste exhaustive des IoCs se trouve dans le fichier « Ranmit\_IoCs.pdf ».**