Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

	Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*