STREAMSCAN

Cybersécurité pour les moyennes entreprises

ANALYSE DU

MALWARE BAD RABBIT

OCTOBRE 2017 //

Introduction

Le mardi 24 Octobre 2017 a connu la propagation d'un nouveau ransomware : "Bad Rabbit". Ce dernier a touché des cibles se situant principalement en Ukraine et en Russie endommageant plusieurs infrastructures.

À l'instar du ransomware WannaCry, 'Bad Rabbit' possède la capacité de se propager sans l'interaction d'un utilisateur ce qui explique le nombre important de machines infectées en peu de temps. StreamScan a publié un livre blanc sur WannaCry. Vous pouvez le consulter à https://www.streamscan.io/fr/2017/Rapport-WannaCrypt0r-FRv1.0.pdf.

Plusieurs experts pensent que ce nouveau ransomware utilise le même mode de propagation que WannaCry, à savoir l'exploitation de la faille EternalBlue. Le fait que le malware Bad Rabbit se mette à scanner le réseau local sur lequel se trouve la machine infectée, à la recherche du service SMB peut en effet laisser croire qu'il utilise EternalBlue. Cette assertion est totalement erronée. Comme, comme nous allons le démontrer dans notre analyse, Bad Rabbit n'exploite pas EternalBlue, mais essaie simplement de se connecter au service SMB en utilisant un dictionnaire de noms d'utilisateurs / mot de passes/ contenu dans son code source.

Analyse dynamique de Bad Rabbit

Nous avons effectué une analyse dynamique de 'Bad Rabbit' dans un environnement de test dans lequel 2 machines Windows 7 sont connectées. La première machine (10.0.1.3) a été infectée avec le ransomware Bad Rabbit alors que la seconde (10.0.1.4) ne l'a pas été. Il est à noter que la deuxième machine est vulnérable à la faille Eternal Blue.

Fichier Bad Rabbit analysé

Nom du fichier malicieux : infpub.dat

Hash MD5 : 1d724f95c61f1055f0d02c2154bbccd3

Résultat de l'analyse dynamique de Bad Rabbit

Nous constatons que dès son infection, la machine 10.0.1.3 se met à scanner le réseau avec des requêtes de diffusion ARP afin de découvrir les hôtes présents (figure 1).

No.	Time	Source	Destination	Protocol	Length	Info
361	405.370603	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.24? Tell 10.0.1.3
362	407.717297	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.25? Tell 10.0.1.3
363	408.370205	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.25? Tell 10.0.1.3
364	409.370844	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.25? Tell 10.0.1.3
365	411.716864	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.26? Tell 10.0.1.3
366	412.370409	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.26? Tell 10.0.1.3
367	413.370656	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.26? Tell 10.0.1.3
368	415.716484	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.27? Tell 10.0.1.3
369	416.370063	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.27? Tell 10.0.1.3
370	417.370581	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.27? Tell 10.0.1.3
371	419.716044	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.28? Tell 10.0.1.3
372	420.370528	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.28? Tell 10.0.1.3
373	421.370342	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.28? Tell 10.0.1.3
374	423.716251	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.29? Tell 10.0.1.3
375	424.370328	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.29? Tell 10.0.1.3
376	425.370039	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.29? Tell 10.0.1.3
377	427.714470	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.30? Tell 10.0.1.3
378	428.372597	PcsCompu_d6:65:52	Broadcast	ARP	42	Who has 10.0.1.30? Tell 10.0.1.3

Figure1. Scan ARP du sous-réseau

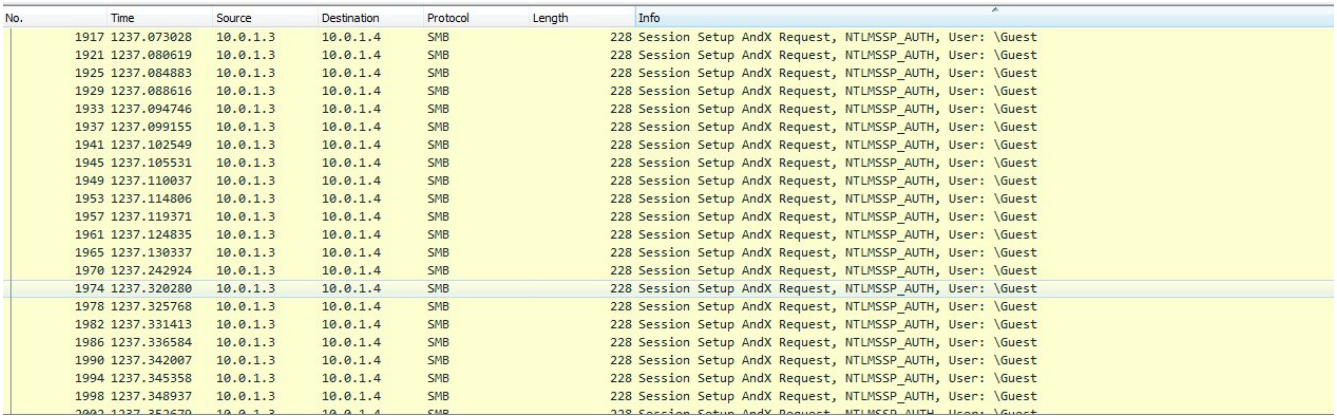
Une fois la seconde machine 10.0.1.4 trouvée, Bad Rabbit essaie de se connecter au service SMB en utilisant différentes combinaisons de noms d'utilisateurs et mots de passes (figures 2,3). Sur la figure 2 ci-dessous, l'on observe les tentatives de connexion via le nom d'utilisateur Admin.

tcp.stream eq 24

No.	Time	Source	Destination	Protocol	Length	Info
1785	1236.898466	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1789	1236.902483	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1793	1236.906285	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1797	1236.910199	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1801	1236.915114	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1805	1236.920234	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1809	1236.924991	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1813	1236.929153	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1817	1236.933166	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1821	1236.936798	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1825	1236.940682	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1829	1236.944723	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1833	1236.948784	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1837	1236.952778	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1841	1236.956599	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1845	1236.960537	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1849	1236.964241	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1853	1236.968126	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1857	1236.971987	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1861	1236.975898	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin
1865	1236.979811	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Admin

Figure 2. Tentative de connexion SMB avec le nom d'utilisateur Admin

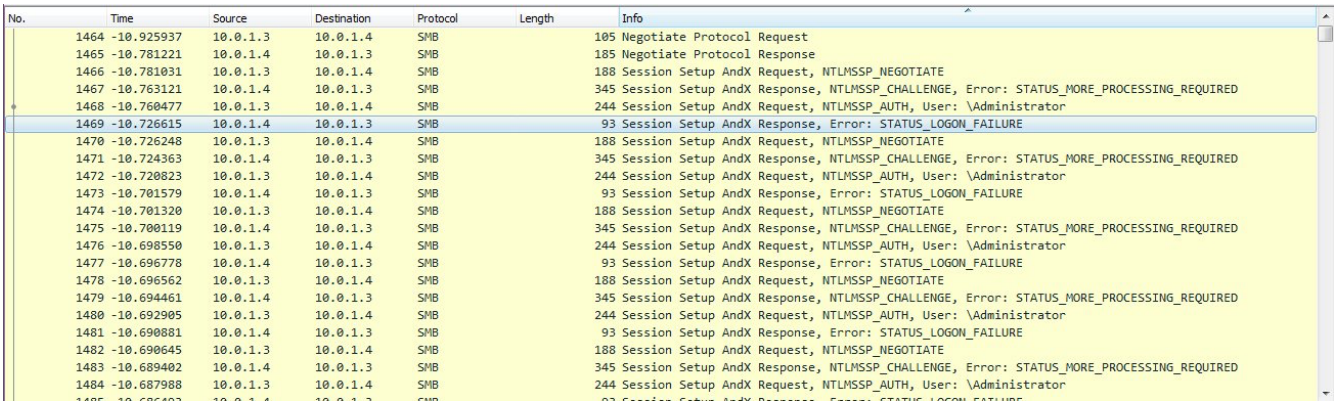
Après l'échec de la tentative de connexion via le nom d'utilisateur **Admin**, un autre nom d'utilisateur est utilisé (ex : **Guest** sur la figure 3). Bad Rabbit essayera de se connecter à la machine 10.0.1.4 en essayant l'ensemble des noms utilisateurs du dictionnaire, dans l'espoir qu'un d'entre autre soit valide. Pour chaque nom d'utilisateur, l'ensemble des mots de passe contenu dans le dictionnaire sera testé.



No.	Time	Source	Destination	Protocol	Length	Info
1917	1237.073028	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1921	1237.080619	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1925	1237.084883	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1929	1237.088616	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1933	1237.094746	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1937	1237.099155	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1941	1237.102549	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1945	1237.105531	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1949	1237.110037	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1953	1237.114806	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1957	1237.119371	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1961	1237.124835	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1965	1237.130337	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1970	1237.242924	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1974	1237.320280	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1978	1237.325768	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1982	1237.331413	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1986	1237.336584	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1990	1237.342007	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1994	1237.345358	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest
1998	1237.348937	10.0.1.3	10.0.1.4	SMB	228	Session Setup AndX Request, NTLMSSP_AUTH, User: \Guest

Figure3. Tentative de connexion SMB avec le nom d'utilisateur Guest

Tous les noms d'utilisateurs et mots de passe du dictionnaire sont essayés et nous constatons que l'attaque échoue (figure 4). Au finish, la deuxième machine (10.0.1.4) n'a pas été infectée.



No.	Time	Source	Destination	Protocol	Length	Info
1464	-10.925937	10.0.1.3	10.0.1.4	SMB	105	Negotiate Protocol Request
1465	-10.781221	10.0.1.4	10.0.1.3	SMB	185	Negotiate Protocol Response
1466	-10.781031	10.0.1.3	10.0.1.4	SMB	188	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1467	-10.763121	10.0.1.4	10.0.1.3	SMB	345	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1468	-10.760477	10.0.1.3	10.0.1.4	SMB	244	Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
1469	-10.726615	10.0.1.4	10.0.1.3	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
1470	-10.726248	10.0.1.3	10.0.1.4	SMB	188	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1471	-10.724363	10.0.1.4	10.0.1.3	SMB	345	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1472	-10.720823	10.0.1.3	10.0.1.4	SMB	244	Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
1473	-10.701579	10.0.1.4	10.0.1.3	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
1474	-10.701320	10.0.1.3	10.0.1.4	SMB	188	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1475	-10.700119	10.0.1.4	10.0.1.3	SMB	345	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1476	-10.698550	10.0.1.3	10.0.1.4	SMB	244	Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
1477	-10.696778	10.0.1.4	10.0.1.3	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
1478	-10.696562	10.0.1.3	10.0.1.4	SMB	188	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1479	-10.694461	10.0.1.4	10.0.1.3	SMB	345	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1480	-10.692905	10.0.1.3	10.0.1.4	SMB	244	Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
1481	-10.690881	10.0.1.4	10.0.1.3	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
1482	-10.690645	10.0.1.3	10.0.1.4	SMB	188	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1483	-10.689402	10.0.1.4	10.0.1.3	SMB	345	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1484	-10.687988	10.0.1.3	10.0.1.4	SMB	244	Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator

Figure4. Échec de la connexion SMB

Le fait que la machine 10.0.1.4 ne soit pas infecté malgré le fait qu'elle soit vulnérable à EternalBlue, confirme que le ransomware Bad Rabbit n'exploite pas cette vulnérabilité.

La machine victime 10.0.1.3 fini par redémarrer et affiche un message (figure 5) indiquant que le contenu de son disque dur est chiffré et que le paiement d'une rançon est exigé pour récupérer ses fichiers.

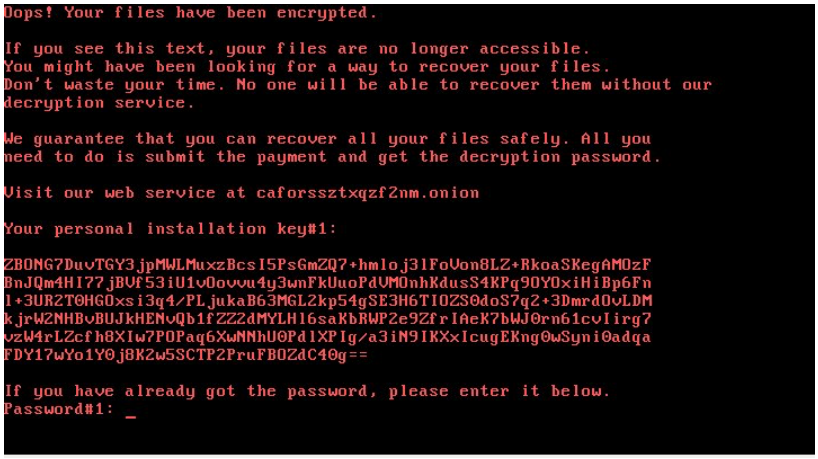


Figure5. Message affiché suite au chiffrement du disque dur de l'ordinateur 10.0.1.3

Observations sur le dictionnaire utilisé par Bad Rabbit

Le dictionnaire utilisé par le ransomware Bad Rabbit pour se propager contient les noms d'utilisateurs ci-dessous.

adminTest	nasuser	support	user-1
user	nas	manager	User1
guest	ftpuser	rdpadmin	User
administrator	asus	rdpuser	Guest
alex	backup	ftp	Admin
netguest	operator	boss	Administrator
superuser	rdp	buh	
ftpadmin	other user	root	
nasadmin	work	Test	

Les mots de passe contenus dans le dictionnaire sont les suivants :

god	qwerty	test123	12345678
sex	test	admin123Test123	1234567
secret	qwert	Admin123	123456

love	qwer	123	12345
321	qwe321	user123	1234
123321	qwe123	User123	
uiop	qwe	guest123	
zxcv	777	Guest123	
zxc321	77777	administrator123	
zxc123	55555	Administrator123	
zxc	111111	1234567890	
qwerty123	password	123456789	

Un mot sur la méthode de propagation de Bad Rabbit

Les noms d'utilisateurs contenus dans le dictionnaire utilisé par Bad Rabbit sont pour la plupart souvent utilisés dans les réseaux informatique (admin, root, etc.) ce qui augmente la probabilité qu'ils soient existants sur les machines sur lesquels Bad Rabbit essaie de se propager. Quant aux mots de passe du dictionnaire, ils sont peu complexes (ex : Administrator123, qwerty123, 77777) et ne devraient à priori pas être utilisés dans le réseau informatique d'une entreprise ou d'une administration gouvernementale. Le mode de propagation de Bad Rabbit n'est donc pas complexe.

La propagation rapide de Bad Rabbit montre à quel point des mots de passe très faibles sont encore utilisés dans les réseaux informatiques.

Recommandations

Les entreprises devraient s'assurer de mettre en place un contrôle d'accès robuste forçant les utilisateurs à utiliser les mots de passe complexes. A cette recommandation s'ajoute la sensibilisation des utilisateurs aux risques de sécurité, la saine gestion des vulnérabilités de sécurité, l'utilisation d'outils de sécurité comportementaux, etc.

StreamScan Détection et Réponse Gérées conçues pour vous

Cet article vous a été présenté par StreamScan. Notre solution de détection et réponse gérées (DRG) combine notre technologie innovante CDS et le soutien de notre équipe de pirates éthiques pour fournir la sécurité réseau dont votre organisation a besoin, à un coût nettement inférieur à celui des frais de licence des logiciels ou de la constitution d'une équipe de sécurité interne.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan MDR peut vous aider à protéger votre entreprise ou votre organisation.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment le DRG de StreamScan peut vous aider à protéger votre entreprise ou votre organisation.

Courriel : demo@streamscan.ai
Téléphone : +1 (650) 264-9702
www.streamscan.ai