Advertencia sobre amenazas cibernéticas de Corea del Norte

Diversas agencias gubernamentales de los Estados Unidos han emitido un comunicado sobre los peligros relacionados con las recientes actividades cibercriminales que está desplegando Corea del Norte. Estas actividades tienen como objetivo afectar la integridad y la estabilidad del sistema financiero internacional. El gobierno de Estados Unidos presenta su preocupación dado que Corea del Norte registra un aumento en sus actividades cibercriminales asociadas al grupo HIDDEN COBRA, las cuales han demostrado que tienen capacidad de afectar infraestructura critica del sector financiero, tal como sucedió en diciembre de 2017 con el ransomware Wannacry 2.0, donde varios países incluido EEUU se vieron afectados y posterior a esto atribuyeron dicho ataque a Corea del Norte.

Publicación:
20/04/2020
Importancia:
Alta
Riesgo de explotación:
Media

Descripción

Actividades contra el sector financiero:

Los actores cibernéticos patrocinados segun agencias gubernamentales de Estados Unidos por la RPDC (Republica Popular de Corea) consisten principalmente en piratas informáticos, criptólogos y desarrolladores de software que realizan espionaje y robo cibernético a instituciones financieras. Desarrollan e implementan una amplia gama de herramientas de malware en todo el mundo para permitir estas actividades, las cuales son cada vez más sofisticadas. Esto ha favorecido la creación de campañas ilícitas como:

-Habilitación de robo financiero cibernetico y lavado de dinero.
-Campañas de extorsión.
-Criptojacking (minería de moneda maliciosa).
-Secuestro de información personal y empresarial.

Historial de campañas conocidas a nivel mundial desplegadas por la RPDC:

-Hackeo a Sony Pictures.
-El golpe contra el Banco de Bangladesh.
-Wannacry 2.0.
-La campaña FAST cash-Hackeo a un exchange de moneda digital

Indicadores de Compromiso

Direcciones IP:

159.100.250.231
188.165.37.168
94.177.123.138
193.56.28.103
107.6.12.135
210.202.40.35
112.175.92.57
113.114.117.122
117.239.241.2
119.18.230.253
128.200.115.228
137.139.135.151
14.140.116.172
181.39.135.126
186.169.2.237
195.158.234.60
197.211.212.59
21.252.107.198
210.137.6.37
217.117.4.110
218.255.24.226
221.138.17.152
26.165.218.44
47.206.4.145
70.224.36.194
81.94.192.10
81.94.192.147
84.49.242.125
97.90.44.200

SHA-256:

04d70bb249206a006f83db39bbe49ff6e520ea329e5fbb9c758d426b1c8dec30
1ea6b3e99bbb67719c56ad07f5a12501855068a4a866f92db8dcdefaffa48a39
618a67048d0a9217317c1d1790ad5f6b044eaa58a433bd46ec2fb9f9ff563dc6
738ba44188a93de6b5ca7e0bf0a77f66f677a0dda2b2e9ef4b91b1c8257da790
b6811b42023524e691b517d19d0321f890f91f35ebbdf1c12cbb92cda5b6de32
133820ebac6e005737d5bb97a5db549490a9f210f4e95098bc9b0a7748f52d1f
43193c4efa8689ff6de3fb18e30607bb941b43abb21e8cee0cfd664c6f4ad97c
fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac
a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442
8ee7da59f68c691c9eca1ac70ff03155ed07808c7a66dee49886b51a59e00085
606c6000f36dc69fefc6df828e1ac9c5529a71a62b99f5df55463606c4c9689c
52f83cdaefd194fff3d387631d5693a709cd7b3a20a072e7827c4d4218d57695
05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461
0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571
084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319
12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676
2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11
4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818
70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33
83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a
8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520
b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9
b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8
d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03
fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5
44a93ea6e6796530bb3cf99555dfb3b1092ed8fb4336bb198ca15b2a21d32980
49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
823d255d3dc8cbc402527072a9220e4c38655de1a3e55a465db28b55d3ac1bf8
96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7
ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09
1ea6b3e99bbb67719c56ad07f5a12501855068a4a866f92db8dcdefaffa48a39
cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f

MD5:

062e9cd9cdcabc928fc6186c3921e945 2d92116440edef4190279a043af6794b
11cb4f1cdd9370162d67945059f70d0d 688890ddbf532a4de7c83a58e6aa594f

Adversarios:

HIDDEN COBRA
STARDUST CHOLLIMA

Referencias:

DPRK Cyber Threat Advisory
Issued: April 15, 2020 Title:
Guidance on the North Korean Cyber Threat

Recomendaciones

- Mantener firmas y motores de antivirus actualizados.
- Mantenga los parches del sistema operativo actualizados.
- Deshabilite los servicios para compartir archivos e impresoras. Si se requieren estos servicios, usar contraseñas seguras o autenticación de Active Directory.
- Restrinja la capacidad de los usuarios (permisos) para instalar y ejecutar aplicaciones de software no deseadas. No agregue usuarios al grupo de administradores locales a menos que sea necesario.
- Tenga cuidado al abrir archivos adjuntos de correo electrónico, incluso si se espera el archivo adjunto y el remitente parece ser conocido.
- Habilite un firewall personal en las estaciones de trabajo configurado para denegar solicitudes de conexión no solicitadas.
- Deshabilite servicios innecesarios en estaciones de trabajo y servidores.
- Buscar y eliminar archivos adjuntos sospechosos de correo electrónico; asegúrese que el archivo adjunto escaneado sea su "tipo de archivo verdadero" (es decir, la extensión coincide con el encabezado del archivo).
- Monitorear los hábitos de navegación web de los usuarios; restringir el acceso a sitios con contenido desfavorable.
- Tenga cuidado al usar medios extraíbles (por ejemplo, unidades de memoria USB, unidades externas, CD, etc.).
- Escanee todo el software descargado de Internet antes de ejecutarlo.
- Mantener una conciencia situacional de las últimas amenazas e implementar listas de control de acceso (ACL) apropiadas.
- Compartir información técnica y hechos históricos sobre las amenazas.
- Asegurar el perímetro de conexiones provenientes de Corea del Norte.
- Inspeccionar profundamente correos de dominios sospechosos o con indicios de relacionamiento con Corea del Norte.
- Notificar a las autoridades competentes de cualquier actividad sospechosa.
- Aplicar el bloqueo en los controles de seguridad acorde a los IoC.
- Generar desde el Monitoreo Inteligente una alerta única temprana (AUT) de ciberseguridad asociada a posibles campañas HIDDEN COBRA y STARDUST CHOLLIMA.

Red Queen Lab Report | DigiSert | Centro de Investigación e Inteligencia de Amenazas | Digiware

#Digiware | #DigiwareSuAliado
#DigiwareSecurity | #DigiwareVisionDay