■ 侵入の痕跡（Indicators of Compromise、IoC）

ファイル詳細	SHA-256	検出名
Payload (CAB)	1fb13a158aff3d258b8f62fe211fabeed03f0763b2acadbccad9e8e39969ea00	Trojan.Win64.COBEACON.SUZ
Exploited Doc	5b85dbe49b8bc1e65e01414a0508329dc41dc13c92c08a4f14c71e3044b06185	Trojan.W97M.CVE202140444.A
Exploited Doc	3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf	Trojan.W97M.CVE202140444.A
Exploited Doc	199b9e9a7533431731fbb08ff19d437de1de6533f3ebbffc1e13eeffaa4fd455	Trojan.W97M.CVE202140444.A
Exploited Doc	938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52	Trojan.W97M.CVE202140444.A
Downloaded JS	d0fd7acc38b3105facd6995344242f28e45f5384c0fdf2ec93ea24bfbc1dc9e6	Trojan.JS.TIVEX.A
Payload (DLL)	6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b	Backdoor.Win64.COBEACON.OSLJAU
Exploited Doc	d0e1f97dbe2d0af9342e64d460527b088d85f96d38b1d1d4aa610c0987dca745	Trojan.W97M.CVE202140444.A
Exploited Doc	a5f55361eff96ff070818640d417d2c822f9ae1cdd7e8fa0db943f37f6494db9	Trojan.W97M.CVE202140444.A

URL	カテゴリ
hxxp://hidusi[.]com/	Malware Accomplice
hxxp://hidusi[.]com/e273caf2ca371919/mountain[.]html	Malware Accomplice
hxxp://hidusi[.]com/94cc140dcee6068a/help[.]html	Malware Accomplice
hxxp://hidusi[.]com/e8c76295a5f9acb7/side[.]html	Malware Accomplice
hxxp://hidusi[.]com/e8c76295a5f9acb7/ministry[.]cab	Malware Accomplice
hxxps://joxinu[.]com	C&C Server
hxxps://joxinu[.]com/hr[.]html	C&C Server
hxxps://dodefoh[.]com	C&C Server
hxxps://dodefoh[.]com/ml[.]html	C&C Server
hxxp://pawevi[.]com/e32c8df2cf6b7a16/specify.html	C&C Server
hxxp://sagoge[.]com/	Malware Accomplice
hxxps://comecal[.]com/	Malware Accomplice
hxxps://rexagi[.]com/	Malware Accomplice
hxxp://sagoge[.]com/get_load	Malware Accomplice
hxxps://comecal[.]com/static-directory/templates[.]gif	Malware Accomplice
hxxps://comecal[.]com/ml[.]js?restart=false	Malware Accomplice
hxxps://comecal[.]com/avatars	Malware Accomplice
hxxps://rexagi[.]com:443/avatars	Malware Accomplice
hxxps://rexagi[.]com/ml[.]js?restart=false	Malware Accomplice
hxxps://macuwuf[.]com	Malware Accomplice
hxxps://macuwuf[.]com/get_load	Malware Accomplice