BLOG ARTICLE

EtterSilent: the underground's new favorite maldoc builder

APR 06, 2021

The cybercrime underground often mimics behaviors that we see in everyday facets of life. Intel 471's latest discovery is an example of one of these patterns: when a product takes off in the marketplace, users will rush to obtain it and find unique ways to use it in order to fit their needs.

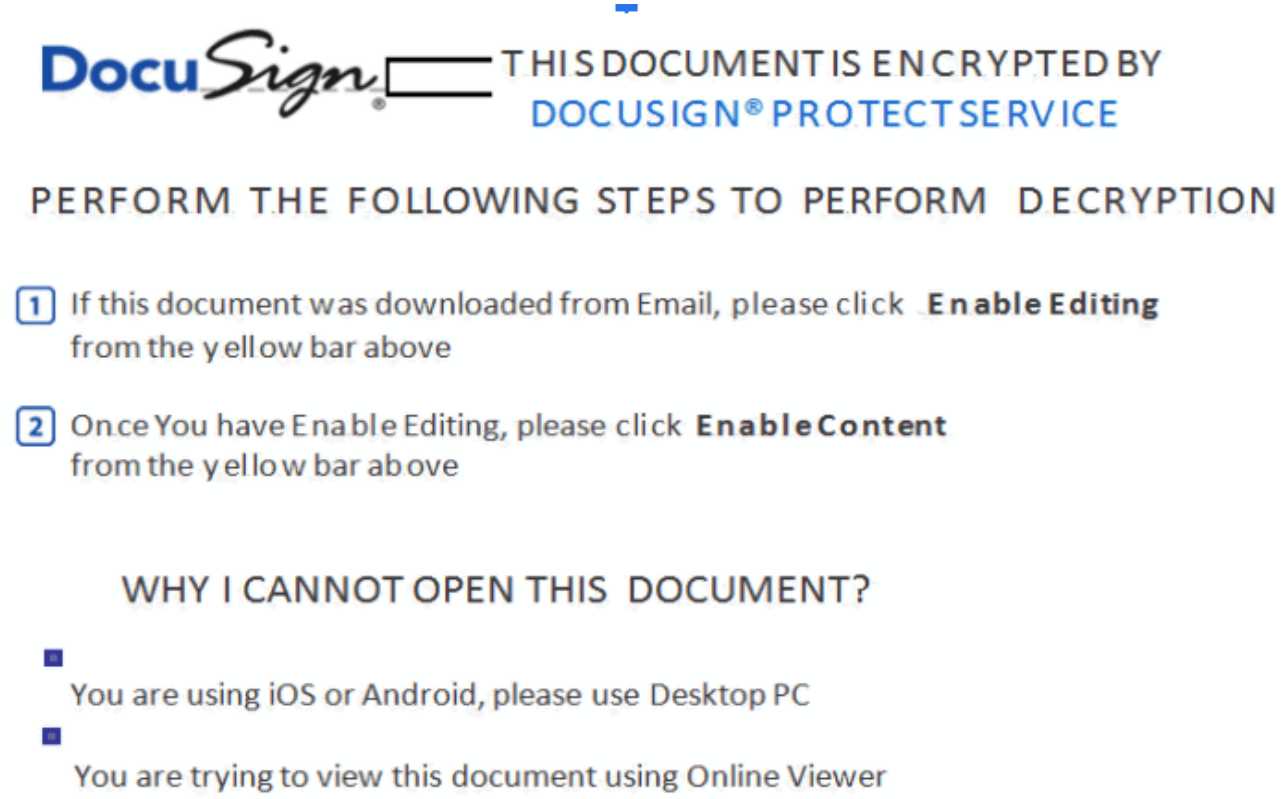
The latest "product" is a malicious document builder, known in the underground as "EtterSilent," that Intel 471 has seen leveraged by various cybercrime groups. As it has grown in popularity, it has constantly been updated in order to avoid detection. Used in conjunction with other forms of malware, it's a prime example of how ease of use and a concentration of skill sets leads to a commoditization of the cybercrime economy.

How it works

First advertised on a well-known Russian cybercrime forum, the seller offered two types of weaponized Microsoft Office documents (maldocs) to users: one that exploits a known vulnerability in Microsoft Office (CVE-2017-8570) and another that uses a malicious macro. To our knowledge, the maldoc with the macro is the more popular choice, possibly due to lower pricing and higher compatibility when compared to the exploit.

The malicious document, when opened, shows a template that poses as DocuSign, the popular software that allows individuals and organizations to electronically sign documents. The maldoc then leverages Excel 4.0 macros stored in a hidden sheet, which allow an externally-hosted payload to be downloaded, written to disk and executed using regsvr32 or rundll32. From there, attackers can follow up and drop

EtterSilent DocuSign template from December 2020



EtterSilent DocuSign template from March 2021

A cybercrime extravaganza

to content

Ettersilent is being used in many malware campaigns, many of which will be familiar to most cybersecurity experts.

It was used in a recent spam campaign to drop an updated version of Trickbot. The maldoc was attached in an email that pretended to be from a well-known multinational appliance manufacturer, claiming to be a payment invoice.

On March 19, 2021, EtterSilent was used as part of a Bazar loader campaign. The analyzed maldoc did not use a DocuSign template, but the main Excel sheet was named "DocuSign®." The maldoc downloads the Bazar payload, which in turn connects to another URL that downloads the related Bazar backdoor.

Everyone needs hosting

Three banking trojans — BokBot, Gozi ISFB and QBot —have also used EtterSilent in conjunction with their schemes. However, what makes these campaigns stand out is their reliance on bulletproof hosting, which is needed to stand up their schemes. All three campaigns use services run by Yalishanda, one of the world's most notorious BPH providers.

Intel 471 tracked a particular campaign tied to BokBot that had numerous distribution URLs embedded in the EtterSilent maldocs. As of the time this blog was published, all of those domains resolved to one particular IP address. That address is tied to bulletproof infrastructure provided by Yalishanda. The usage of Yalishanda's BPH service specifically for the delivery URL is reminiscent of years worth of Hancitor campaigns observed by Intel 471.

We have written extensively how bulletproof hosting works hand-in-glove with cybercrime for decades, supplying criminals with the infrastructure they need to carry out their crimes. EtterSilent's attachment to Yalishanda is another example of that notion.

A piece in a bigger puzzle

The widespread use of EtterSilent shows how commoditization is a big part of the cybercrime economy. Different players specialize in their respective area, whether that be robust hosting, spam infrastructure, maldoc builders, or malware as a service, and find ways to leverage each other's products in services by working [illegible] a better understanding of not only the malware being used, but how the

Appendix 1 - Indicators of compromise

Description	Value
Trickbot payload	9118198afca6e2479fdbcca55a08a4408570d2186a7dd8f261f1821178deb595
Trickbot distribution URL	http://costacars[.]es/ico/ortodox.php
EtterSilent maldoc	50fd4b2e51908a55f2c891fb3ffde2c3661e4324c1887e65fabfb1a93a41efb2
IcedID payload	8e51ccc6c8d14f0365d2d597c8aaf6015238839c0dab90e419107782bf460414
IcedID distribution URL	http://188[.]127.254.114/44270.7082388889.dat
EtterSilent maldoc	2baf563da8db9e2ed765fa7697025d277d06ee53424f6513671f2f6b7441387b
QBot payload	24753d9f0d691b6d582da3e301b98f75abbdb5382bb871ee00713c5029c56d44
Qbot distribution URL	
EtterSilent maldoc	16a0c2f741a14c423b7abe293e26f711fdb984fc52064982d874bf310c520b12
Ursnif payload	d5b05a81f377c33a2fba292002d0474b68483225aa09c97a00336fc368383d6a
Ursnif distribution URL	
EtterSilent maldoc	267a54f074b688d591d5cfb7831f1adb443ec1441076775cb158bed0d385f712
Bazar payload	b7ce29ffbdf00771b539b28ce01d57cd5805ca3a6ca2eb1b694eed4466912286

Skip to content

EtterSilent maldoc	5f8e3b19cd4d25ac396cf64f6f448d88e301cf899142bdb03a28cec42eb71389
Qbot payload	6a984d3aaffeeec32f3803489c71bfd907e2fb74dbc8eeb931c084f11293e1cc
Qbot distribution URL	http://pokojewewladyslawowie[.]pl/orlpzhiy/44270.5684626157.dat
EtterSilent maldoc	3a5d67bdc42b7a9ebd1137e49a34d82c0ee99343ae32f3367137db19131c2cf4
Trickbot payload	aa40f9dd1212993f79cc23111de3a8dd5e529dd1a8ca5dceaa30fba53f6f96b4
Trickbot distribution URL	http://mineiro[.]ch/casrtnoar/count.php
EtterSilent maldoc	9b1c03b0cca23a94f2d6988c66eb0d246ec2648623765e83dbf20548ac874837
Ursnif payload	1c65c1a53f1cf5372bb35b5af5130e966b4bb7e7941cc1460f28628249ce5189
Ursnif distribution URL	
EtterSilent maldoc	2a3316b69ec787ca13a3e35697bcfc4a5e37a9a3080434c56fdf17e0593e0a12

to content