DBGer Ransomware Uses EternalBlue and Mimikatz to Spread Across Networks

bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/

Catalin Cimpanu

By
Catalin Cimpanu

- June 14, 2018
- 01:40 PM
- 0

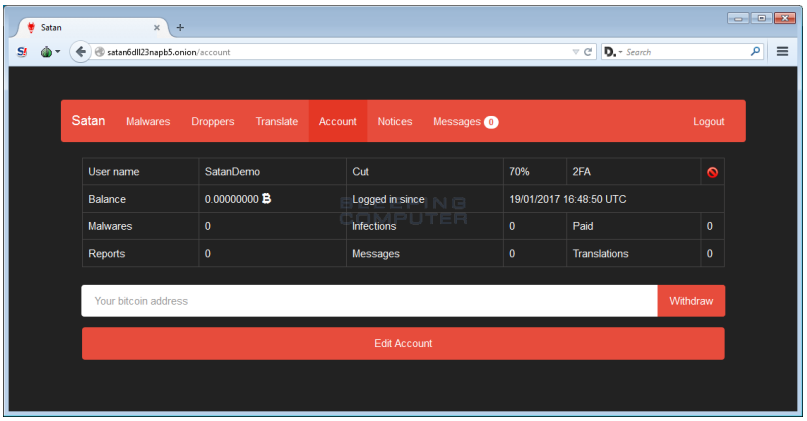
The authors of the Satan ransomware have rebranded their "product" and they now go by the name of DBGer ransomware, according to security researcher MalwareHunter, who spotted this new version earlier today.

The change was not only in name but also in the ransomware's modus operandi. According to the researcher, whose discovery was later confirmed by an Intezer code similarity analysis, the new (Satan) DBGer ransomware now also incorporates Mimikatz, an open-source password-dumping utility.

The purpose of DBGer incorporating Mimikatz is for lateral movement inside compromised networks. This fits a recently observed trend in Satan's modus operandi.

History of Satan ransomware

The Satan ransomware launched in January 2017 as a Ransomware-as-a-Service (RaaS) portal, allowing anyone to register and create custom versions of the Satan ransomware.



First versions were unsophisticated, as most new ransomware variants tend to be. For a long time, the Satan crew rented its ransomware to other crooks, who then distributed it to victims, mostly via email spam (malspam) campaigns.

With time, the ransomware gained a lot of reputation and clients on the criminal underground. The group behind the LockCrypt ransomware started as Satan RaaS customers before developing their own strain. Further, other ransomware devs took inspiration from the Satan code, such as the Iron ransomware group.

Satan devs learn from the WannaCry outbreak

But the Satan crew didn't stand idly either. As the ransomware scene evolved in 2017, they evolved as well.

Changes in the ransomware scene of 2017 included self-spreading mechanisms (seen in the three ransomware outbreaks of last year) and a move to infecting larger networks instead of home users (because of larger payouts and payout rate).

Around November 2017, Satan devs started their plans of updating the ransomware to better fit these trends.

The first step they took was to incorporate a version of the EternalBlue SMB exploit. The addition of this exploit meant that after Satan infected a computer, the ransomware would use EternalBlue to scan the local network for computers with outdated SMB services and infect them as well, maximizing an attack's impact.

This mechanism has been previously analyzed by security researcher Bart Parys in a blog post here.

Other ransomware strains that used EternalBlue included WannaCry, NotPetya, and UIWIX, and all used it in a similar way.

Satan ransomware also adds exploits

This focus on bolstering a lateral movement system continued in 2018, as the ransomware received another update to its lateral movement mechanism at the start of May.

AlienVault experts noticed that new versions of Satan would also scan local networks and attempt to infect other computers using one of the below exploits/methods:

JBoss CVE-2017-12149
Weblogic CVE-2017-10271
Tomcat web application brute forcing

DBGer adds Mimikatz

The new (Satan) DBGer ransomware strain continues this focus on lateral movement. The new version spotted today works by dropping Mimikatz, dumping passwords for networked computers, and using these credentials to access and infect those devices as well.

The development path we see taken by the Satan/DBGer crew is what we can expect in the coming months from most ransomware strains.

Cybercrime gangs have understood by now that there is more money to be made from coin-mining campaigns rather than ransomware. The groups who are still active on the ransomware scene will need to improve their code to maximize profits and adding self-spreading and lateral movement mechanisms is the simplest way to do that.

This is because self-spreading and lateral movement features in ransomware allow a crook the opportunity to infect and receive multiple ransom payments just by fooling one absent-minded employee to open a boobytrapped file.

IOCs:

Sha256: 1f3509cc11ffa1f7d839df93615cf1ba0819d75cafd5ef59110d9b01fb90addd

Modification to file extensions:
image.png -- > [dbger@protonmail.com]image.png.dbger

Ransom note:

_How_to_decrypt_files.txt

```
Some files have been encrypted
Please send ( 1 ) bitcoins to my wallet address
If you paid, send the machine code to my email
I will give you the key
If there is no payment within three days,
we will no longer support decryption
If you exceed the payment time, your data will be open to the public download
We support decrypting the test file.
Send three small than 3 MB files to the email address

BTC Wallet : [redacted]
Email: dbger@protonmail.com
Your HardwareID:
```

```
Some files have been encrypted
Please send ( 1 ) bitcoins to my wallet address
If you paid, send the machine code to my email
I will give you key
If there is no payment within three days,
we will no longer support decryption
If you exceed the payment time, your data will be open to the public download
We support decrypting the test file.
send three small than 3 MB files to the email address

部分文件已经被加密
发送 ( 1 ) 个比特币到我的钱包
付款之后， 把你的硬件ID发送到我的邮件
我们将回复给你解密钥匙
如果在三天内没有支付
我们将不再支持解密
如果您超过付款时间 您的数据将会公开下载
我们支持解密测试文件
发送三个小于 3 MB的文件到邮件

일부 파일이 암호화되었습니다
내 지갑 주소로 ( 1 ) 비트 동전을 보내주세요
이미 지불 한 경우 ,하드웨어 를 내 이메일로 보내주십시오
내가 너에게 비밀 번호를 줄 것이다
3 일 이내에 지불이 완료되지 않으면
더 이상 암호 해독을 지원하지 않습니다
지불 시간을 초과하면 데이터는 일반인에게 공개됩니다
테스트 파일의 암호 해독을 지원합니다
이메일 주소에 3MB 미만의 파일 세 개를 보냅니다

BTC Wallet :3EbN7FP8f8x9FPQQoJKXvyoHJgSkKmAHPY
Email:dbger@protonmail.com
Your HardwareID: [redacted]
```

- DBGer
- ETERNALBLUE
- Mimikatz
- Ransomware
- Satan

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May

2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: