Quick Heal

Indian Power Sector targeted with latest LockBit 3.0 variant

By Quick Heal

AVAR 2022

Meet the Expert

Quick Heal

Sathwik Ram Prakki

Security Researcher

Experience

- Security Researcher at Quick Heal Security Labs
- Cyber Security Engineer at C-DAC

Work

- Threat Intelligence
- Threat Hunting
- Malware Analysis
- Offensive Security

Agenda

Quick Heal

- Targeting Operational Technology
- Threat Landscape and Prominent Attacks
- Conti group's Demise
- LockBit Black – Evolution of RaaS
- Adopting New Tactics
- Conclusion

Targeting Operational Technology

MANUFACTURING

TRANSPORTATION

POWER AND ENERGY

OIL AND GAS

WATER

Threat Landscape

Quick Heal

Top Attack Types

- Ransomware
- Remote Access Trojan
- Server Access
- DDoS
- Web-Script and Worms

Top Infection Vectors

- Vulnerability Exploitation
- Stolen Credentials
- Phishing
- Removable Media
- Brute Force

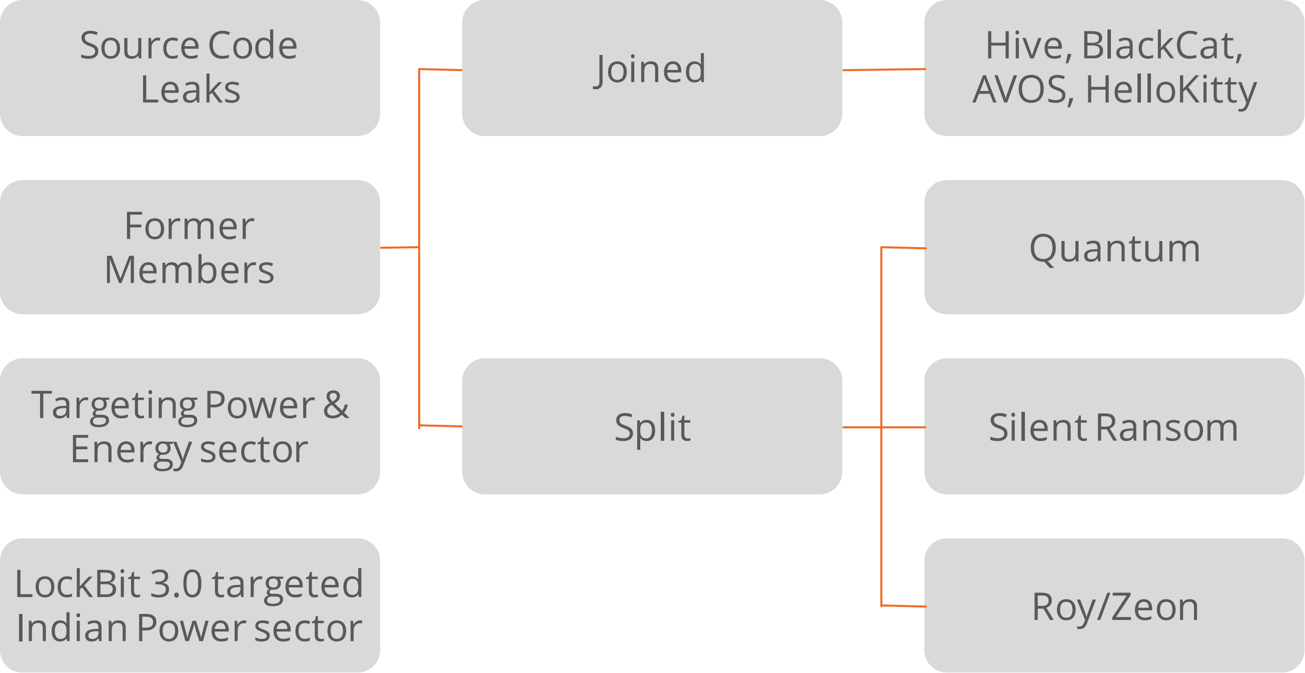
Ransomware Attacks on OT Industry

Quick Heal

Timeline of prominent attacks

Ransomware Group	Target Sector	Target Company	Month
Pandora	Manufacturing	Toyota, Denso	February
RansomExx	Healthcare	Scottish Assoc. For Mental Health	March
LockBit	Manufacturing	Foxconn	May
Quantum	Education	Glenn County Office	June
Black Basta	Manufacturing	Knauf Group	June
BlackCat	Power, Energy and Gas	European Gas Pipeline	July
		Italy's Energy Agency	August
		Creos Luxemborg	
LV	Manufacturing	Semikron	August
Ragnar Locker	Energy, Airlines	DESFA, TAP Air Portugal	August

Conti Group's Demise



Source Code Leaks

Former Members

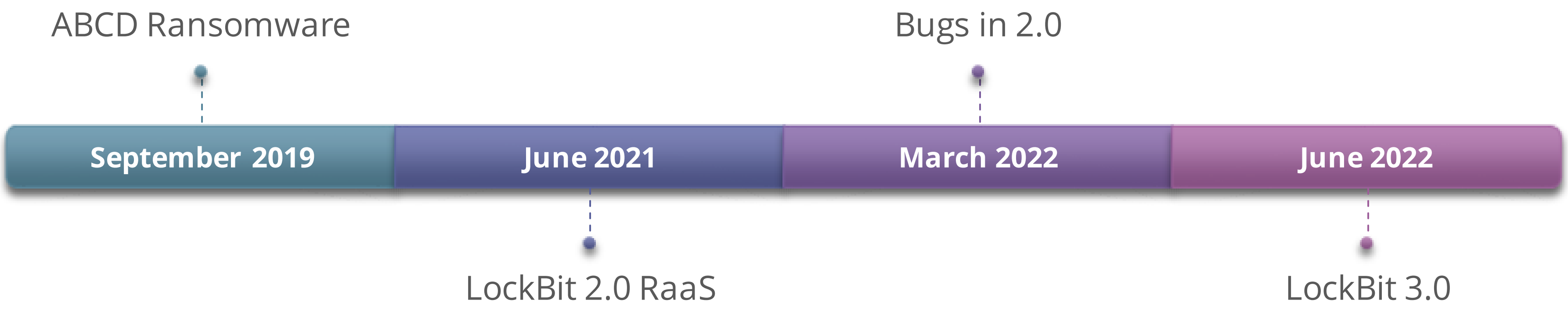
- Joined
  - Hive, BlackCat, AVOS, HelloKitty
- Split
  - Quantum
  - Silent Ransom
  - Roy/Zeon

Targeting Power & Energy sector

LockBit 3.0 targeted Indian Power sector

CONTI

LockBit Black – Evolution of RaaS



ABCD Ransomware

September 2019

June 2021

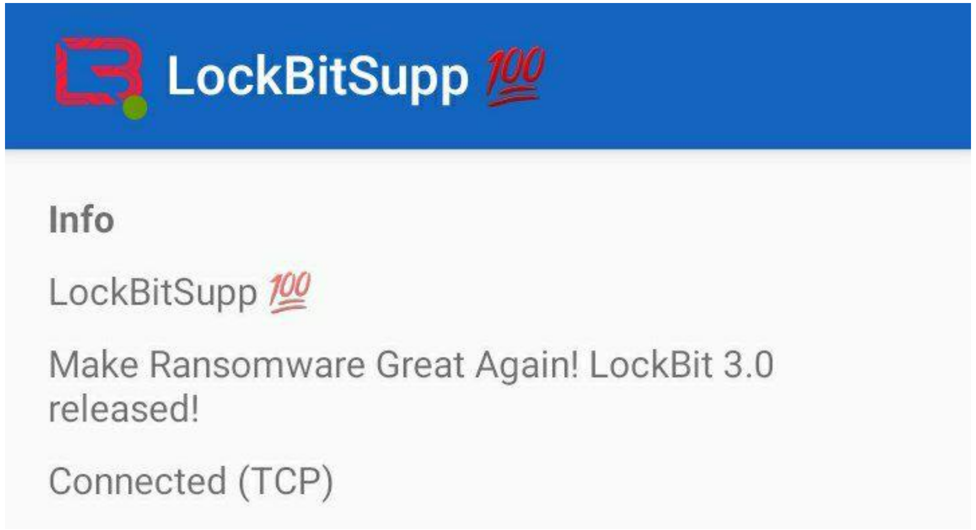
LockBit 2.0 RaaS

Bugs in 2.0

March 2022

June 2022

LockBit 3.0



LockBitSupp 💯

Info

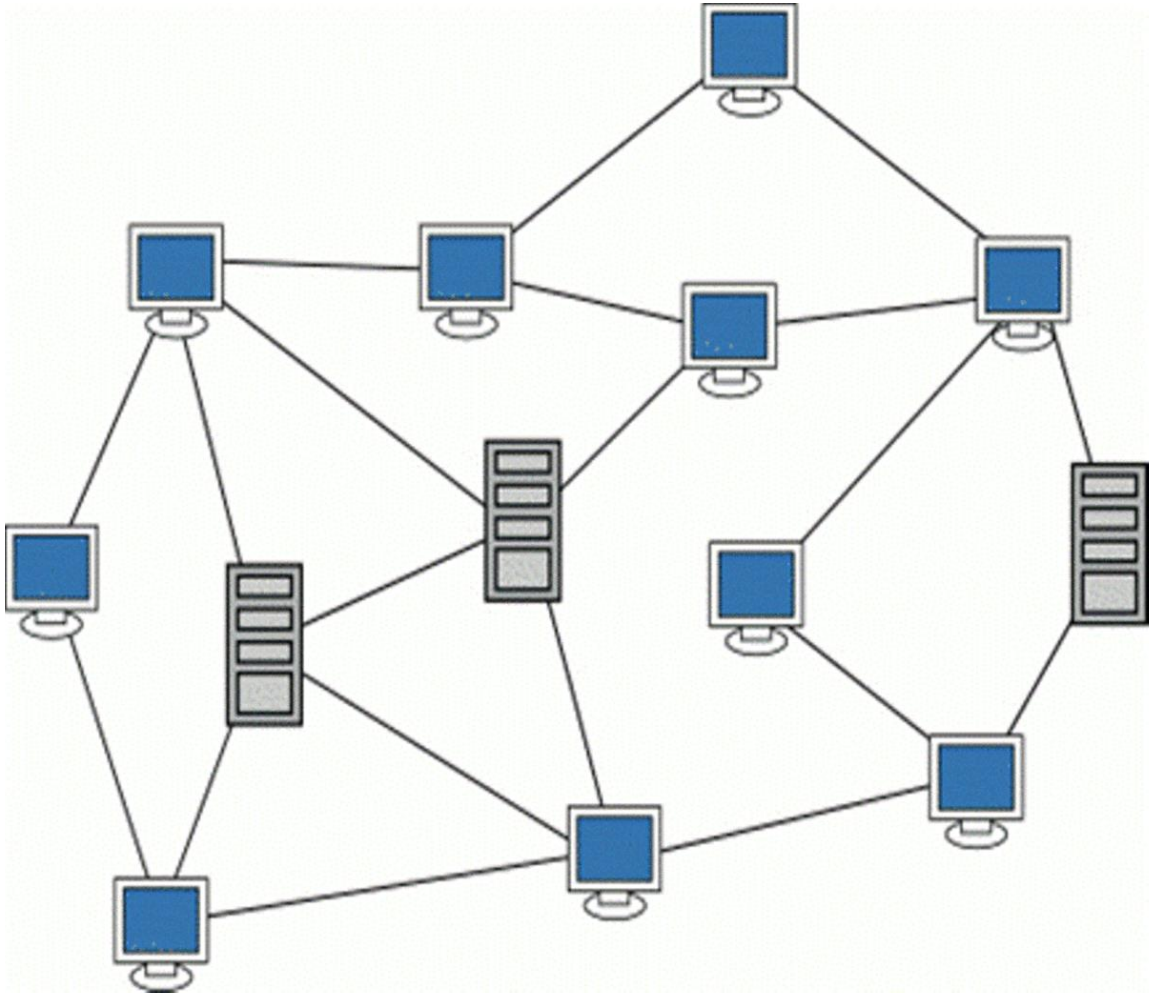
LockBitSupp 💯

Make Ransomware Great Again! LockBit 3.0 released!

Connected (TCP)

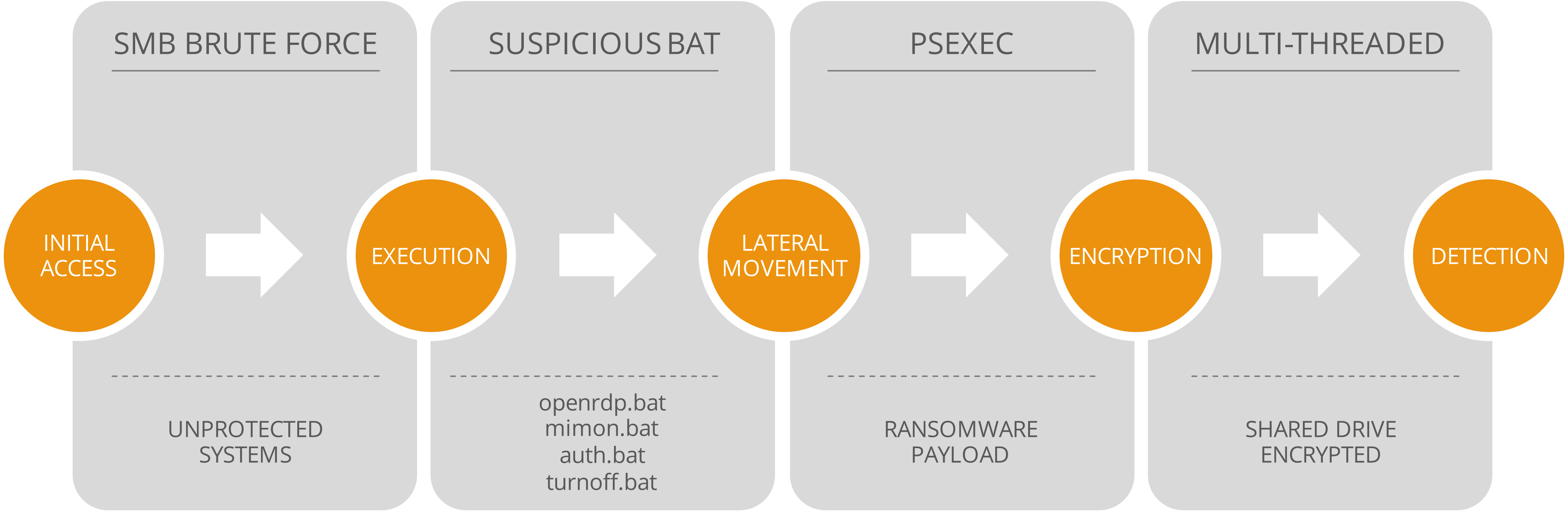
Initial Analysis

- Endpoints at multiple locations
- Encryption in **June-2022**
- Brute Force Attacks



Attack Chain

Quick Heal



SMB BRUTE FORCE

INITIAL ACCESS

UNPROTECTED SYSTEMS

SUSPICIOUS BAT

EXECUTION

openrdp.bat
mimon.bat
auth.bat
turnoff.bat

PSEXEC

LATERAL MOVEMENT

RANSOMWARE PAYLOAD

MULTI-THREADED

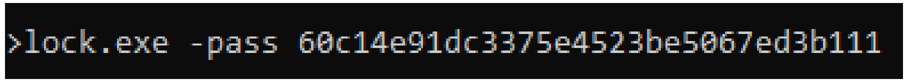
ENCRYPTION

SHARED DRIVE ENCRYPTED

DETECTION

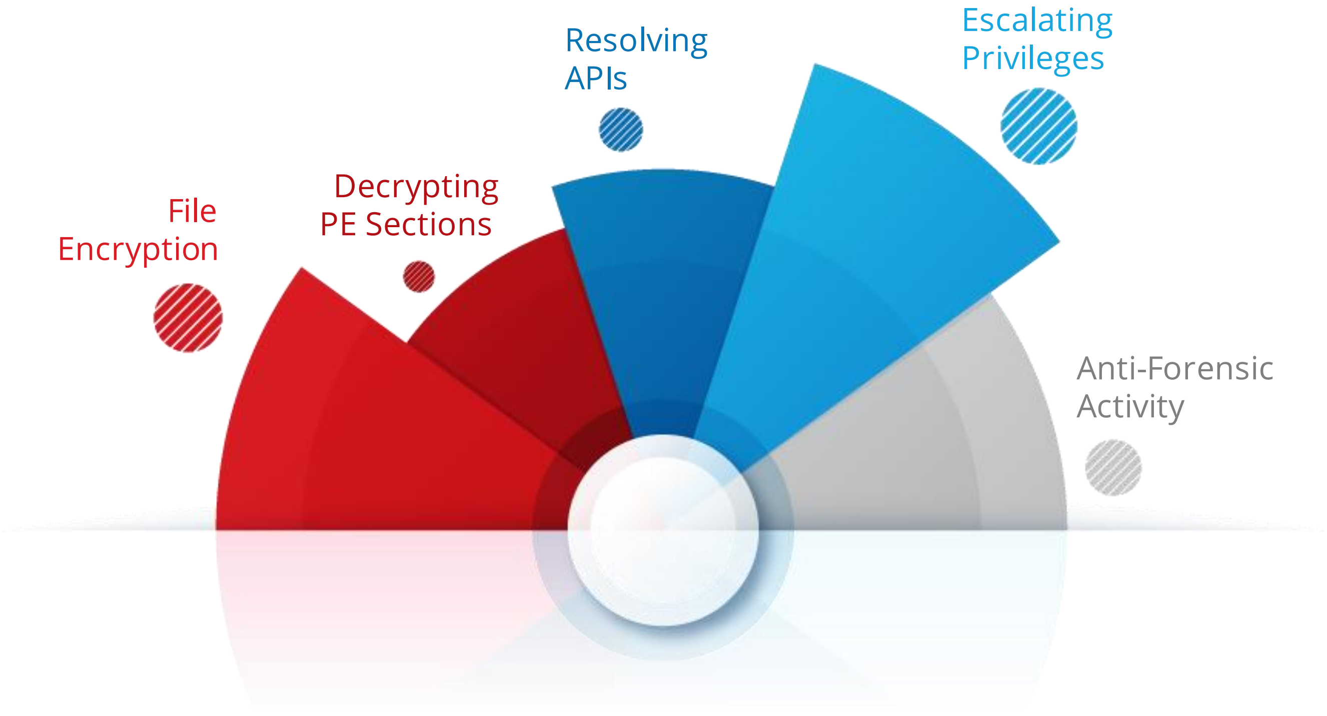
Payload Analysis

- ▶ Dropped in Windows directory
- ▶ Execution requires pass key

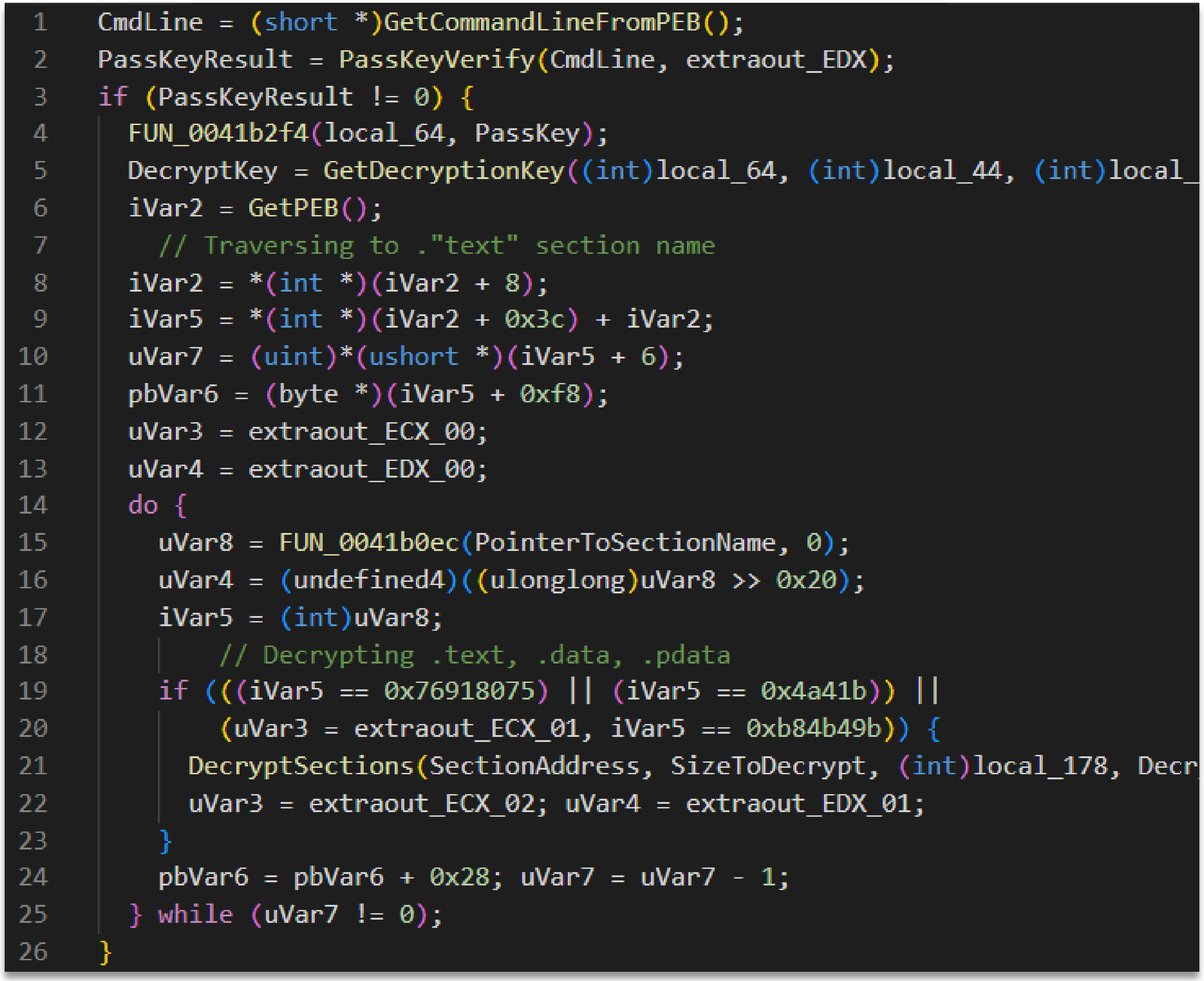


```
>lock.exe -pass 60c14e91dc3375e4523be5067ed3b111
```

  - ◆ Egregor
  - ◆ BlackCat



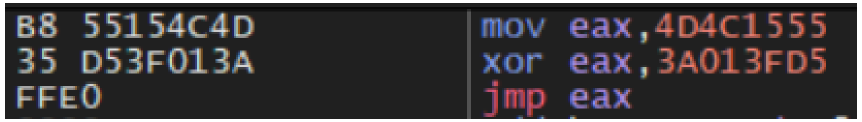
Decrypting Specific Sections



```
CmdLine = (short *)GetCommandLineFromPEB();
PassKeyResult = PassKeyVerify(CmdLine, extraout_EDX);
if (PassKeyResult != 0) {
  FUN_0041b2f4(local_64, PassKey);
  DecryptKey = GetDecryptionKey((int)local_64, (int)local_44, (int)local_
  iVar2 = GetPEB();
    // Traversing to ."text" section name
  iVar2 = *(int *)(iVar2 + 8);
  iVar5 = *(int *)(iVar2 + 0x3c) + iVar2;
  uVar7 = (uint)*(ushort *)(iVar5 + 6);
  pbVar6 = (byte *)(iVar5 + 0xf8);
  uVar3 = extraout_ECX_00;
  uVar4 = extraout_EDX_00;
  do {
    uVar8 = FUN_0041b0ec(PointerToSectionName, 0);
    uVar4 = (undefined4)((ulonglong)uVar8 >> 0x20);
    iVar5 = (int)uVar8;
        // Decrypting .text, .data, .pdata
    if (((iVar5 == 0x76918075) || (iVar5 == 0x4a41b)) ||
        (uVar3 = extraout_ECX_01, iVar5 == 0xb84b49b)) {
      DecryptSections(SectionAddress, SizeToDecrypt, (int)local_178, Decr
      uVar3 = extraout_ECX_02; uVar4 = extraout_EDX_01;
    }
    pbVar6 = pbVar6 + 0x28; uVar7 = uVar7 - 1;
  } while (uVar7 != 0);
}
```

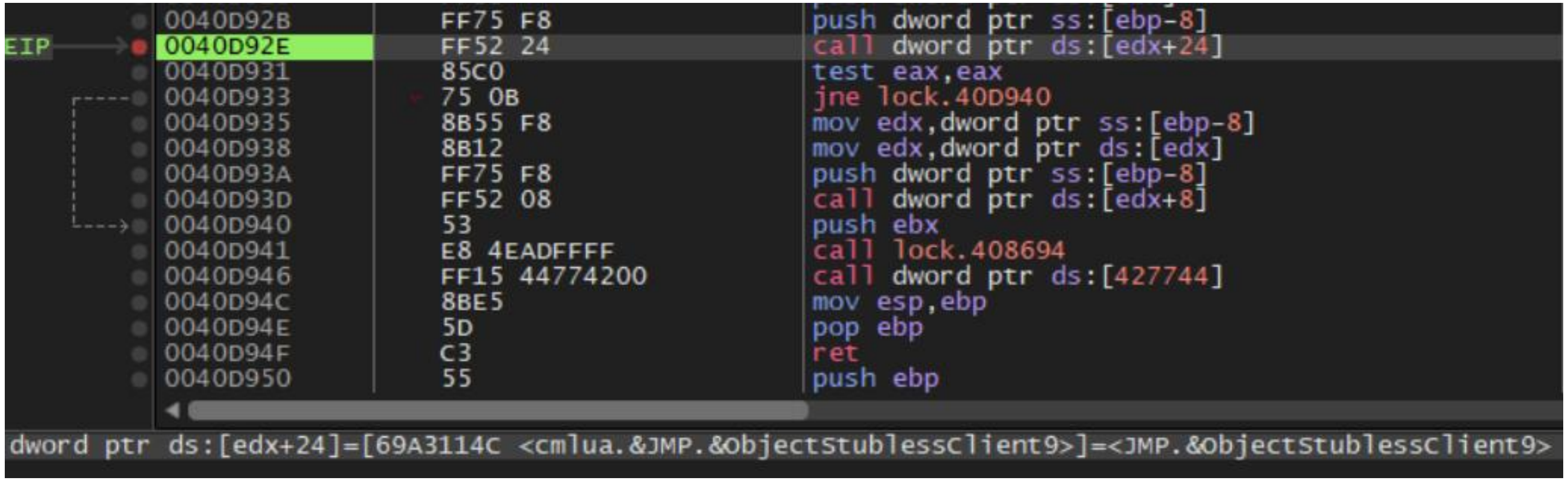
Resolving APIs and Escalating Privileges

- Dynamic Resolution of Win32 APIs



```
B8 55154C4D          mov eax,4D4C1555
35 D53F013A          xor eax,3A013FD5
FFE0                 jmp eax
```

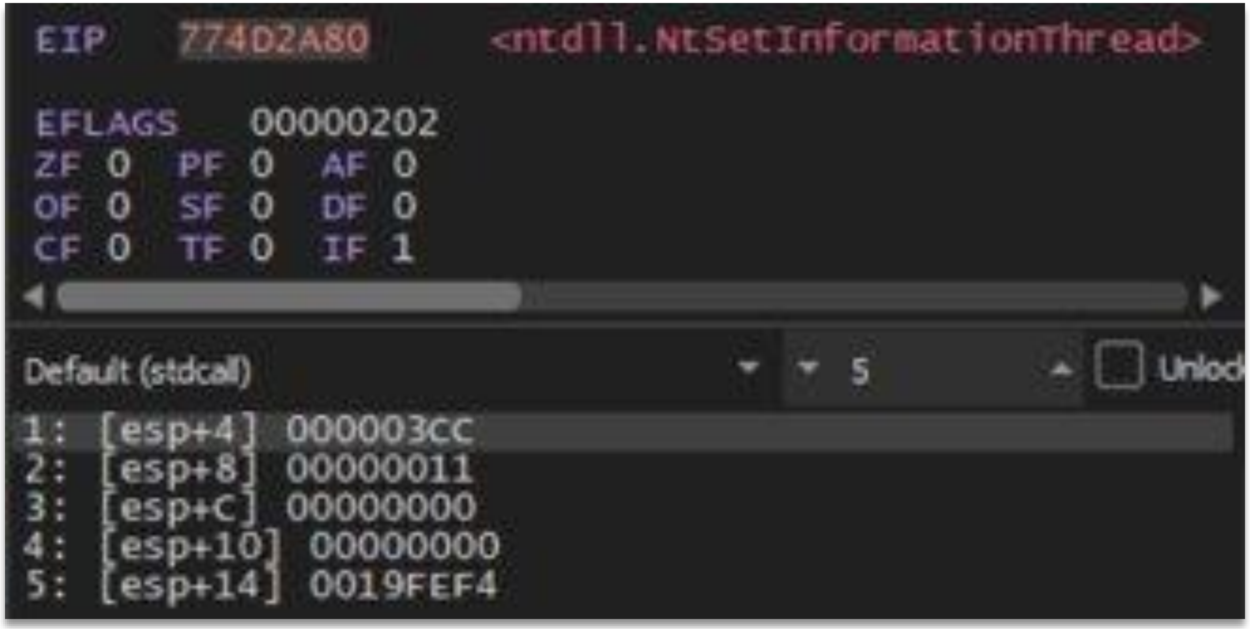
- Privilege Escalation – CMSTPLUA COM (UAC Bypass)



```
        0040D92B     FF75 F8          push dword ptr ss:[ebp-8]
EIP --> 0040D92E     FF52 24          call dword ptr ds:[edx+24]
        0040D931     85C0             test eax,eax
   ┌--- 0040D933     75 0B            jne lock.40D940
   |    0040D935     8B55 F8          mov edx,dword ptr ss:[ebp-8]
   |    0040D938     8B12             mov edx,dword ptr ds:[edx]
   |    0040D93A     FF75 F8          push dword ptr ss:[ebp-8]
   |    0040D93D     FF52 08          call dword ptr ds:[edx+8]
   └--> 0040D940     53               push ebx
        0040D941     E8 4EADFFFF      call lock.408694
        0040D946     FF15 44774200    call dword ptr ds:[427744]
        0040D94C     8BE5             mov esp,ebp
        0040D94E     5D               pop ebp
        0040D94F     C3               ret
        0040D950     55               push ebp

dword ptr ds:[edx+24]=[69A3114C <cmlua.&JMP.&ObjectStublessClient9>]=<JMP.&ObjectStublessClient9>
```

Anti-debugging

- Threads Hidden from Debugger
- **NtSetInformationThread**
  - THREAD_INFORMATION_CLASS::ThreadHideFromDebugger



```
EIP    774D2A80      <ntdll.NtSetInformationThread>

EFLAGS     00000202
ZF  0   PF  0   AF  0
OF  0   SF  0   DF  0
CF  0   TF  0   IF  1
```

Default (stdcall) ▾ ▾ 5 ▴ □ Unlock

```
1:  [esp+4]  000003CC
2:  [esp+8]  00000011
3:  [esp+C]  00000000
4:  [esp+10]  00000000
5:  [esp+14]  0019FEF4
```

Anti-forensic Activity

Quick Heal

01

Clearing Event Logs

02

Deleting Services

03

Killing Tasks

04

Terminating Processes

05

Deleting Volume Shadow Copies

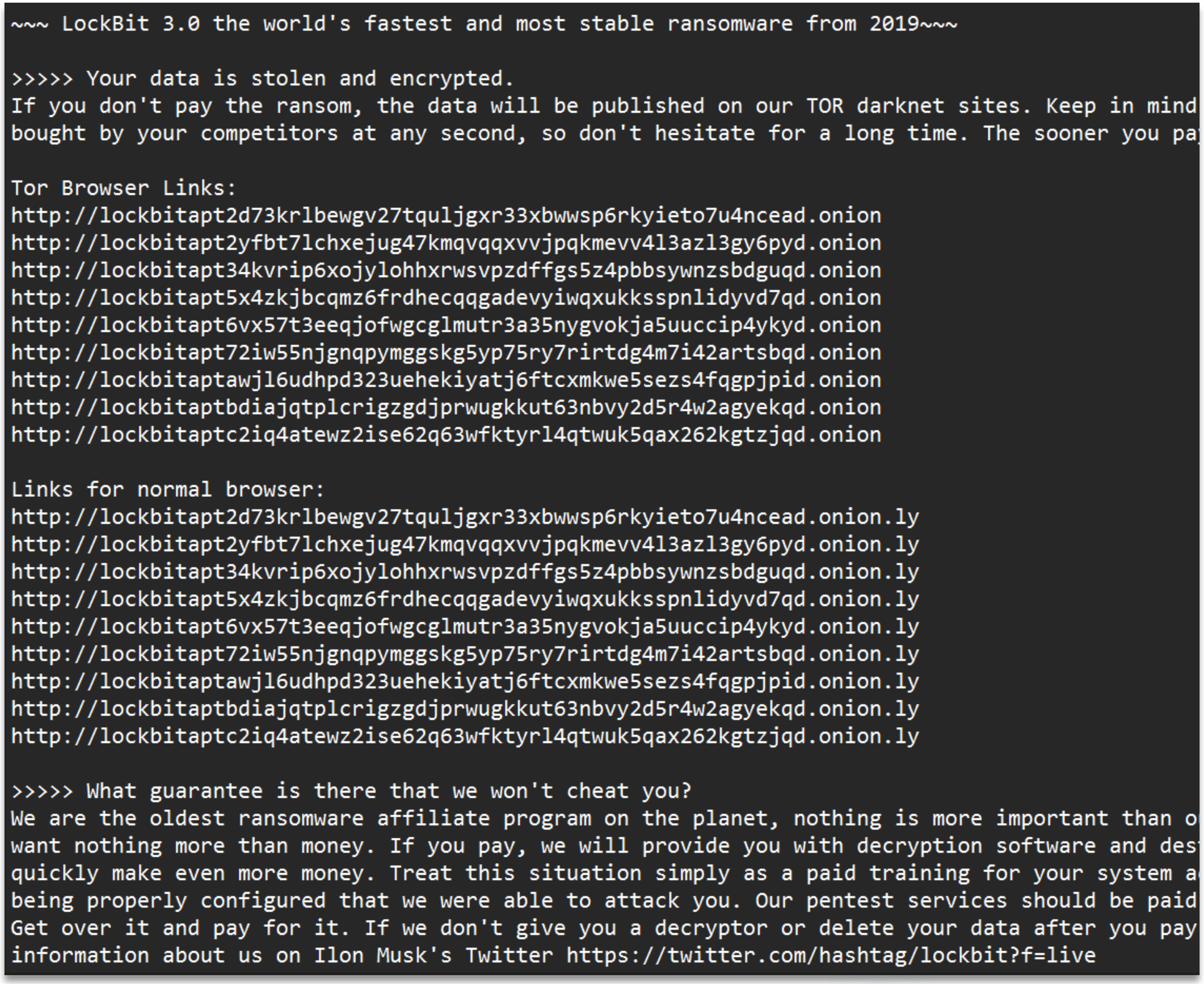
06

Removing Active Network Connections

Ransom Note

Quick Heal

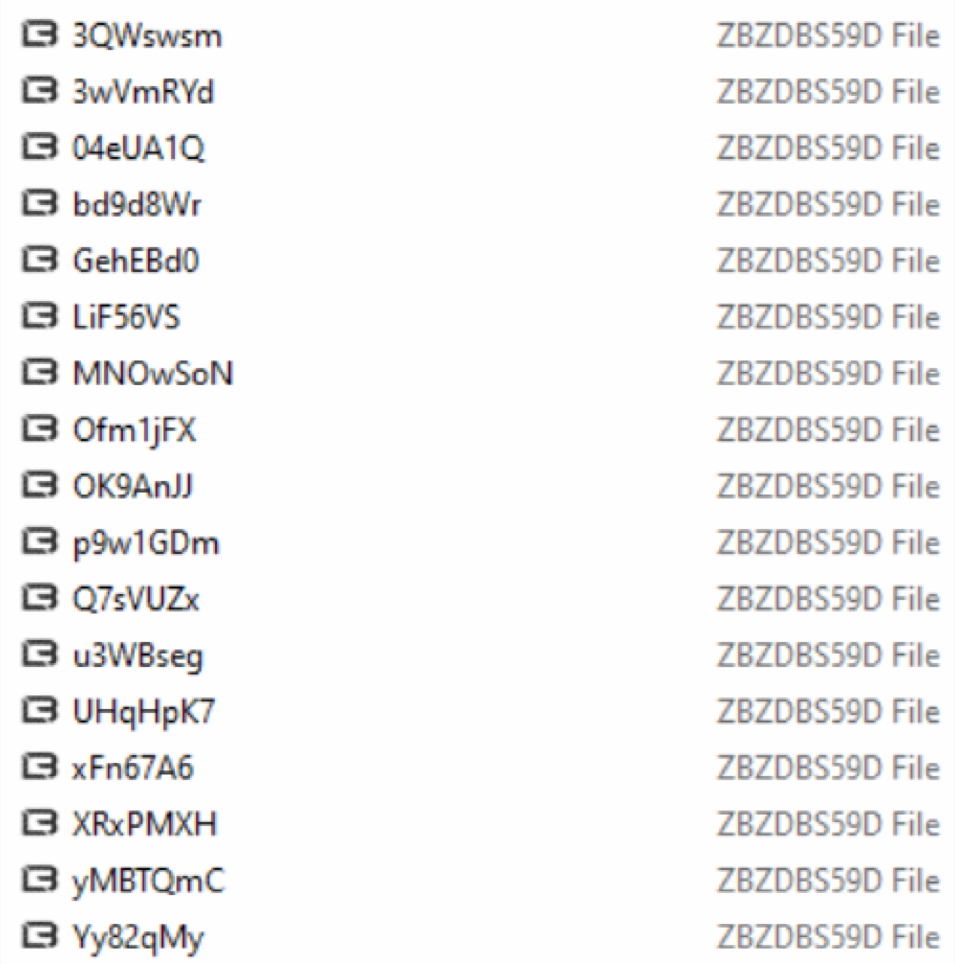
- Zbzdbs59d.README.txt
- Personal ID
- TOR Mirrors



```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind
bought by your competitors at any second, so don't hesitate for a long time. The sooner you pa

Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than o
want nothing more than money. If you pay, we will provide you with decryption software and des
quickly make even more money. Treat this situation simply as a paid training for your system a
being properly configured that we were able to attack you. Our pentest services should be paid
Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay
information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live
```

File Encryption

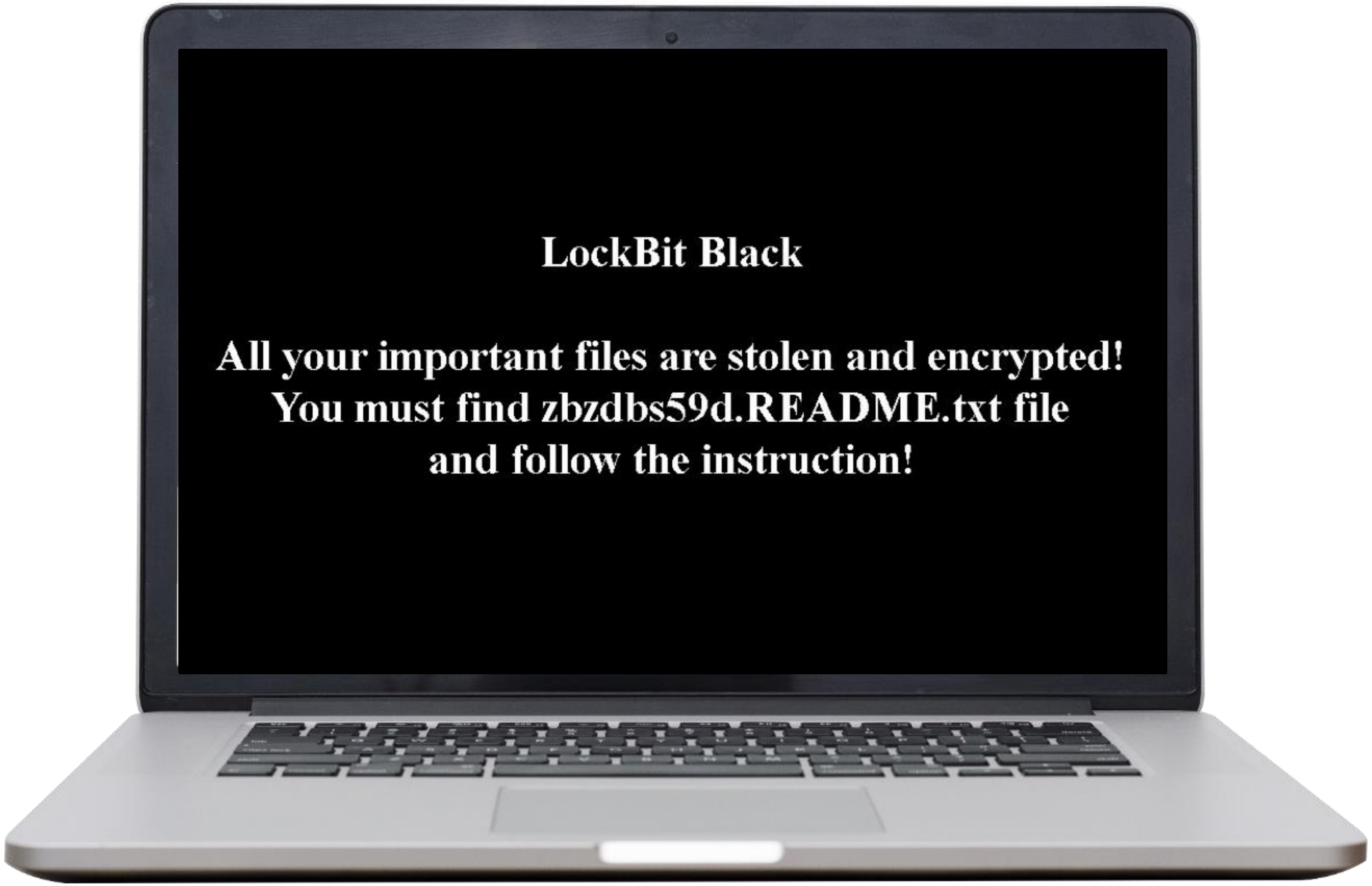
- ✓ File Icon in *ProgramData*
- Renaming files randomly
- Full encryption in 2 mins



3QWswsm	ZBZDBS59D File
3wVmRYd	ZBZDBS59D File
04eUA1Q	ZBZDBS59D File
bd9d8Wr	ZBZDBS59D File
GehEBd0	ZBZDBS59D File
LiF56VS	ZBZDBS59D File
MNOwSoN	ZBZDBS59D File
Ofm1jFX	ZBZDBS59D File
OK9AnJJ	ZBZDBS59D File
p9w1GDm	ZBZDBS59D File
Q7sVUZx	ZBZDBS59D File
u3WBseg	ZBZDBS59D File
UHqHpK7	ZBZDBS59D File
xFn67A6	ZBZDBS59D File
XRxPMXH	ZBZDBS59D File
yMBTQmC	ZBZDBS59D File
Yy82qMy	ZBZDBS59D File

Changing Wallpaper

Quick Heal

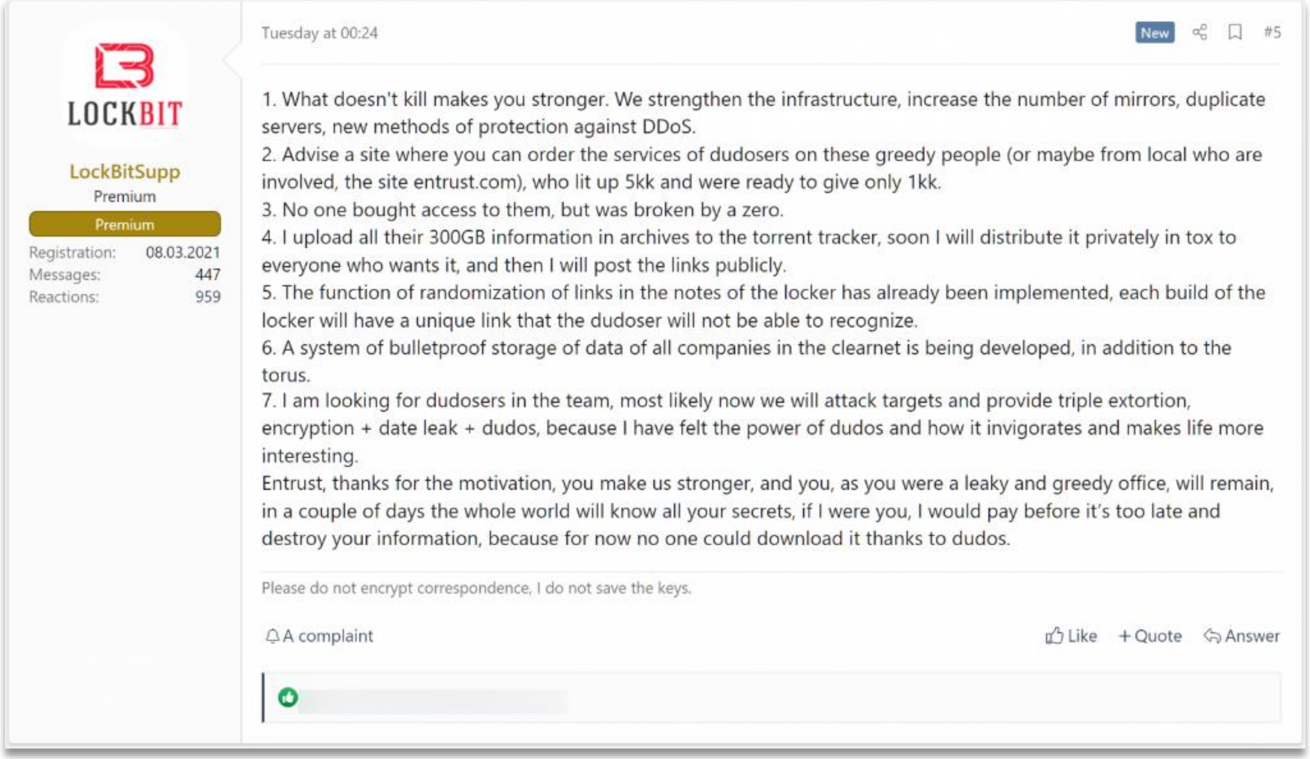


LockBit Black

All your important files are stolen and encrypted!
You must find zbzdbs59d.README.txt file
and follow the instruction!

Adopting New Tactics

Quick Heal



Registration: 08.03.2021
Messages: 447
Reactions: 959

Tuesday at 00:24

1. What doesn't kill makes you stronger. We strengthen the infrastructure, increase the number of mirrors, duplicate servers, new methods of protection against DDoS.
2. Advise a site where you can order the services of dudosers on these greedy people (or maybe from local who are involved, the site entrust.com), who lit up 5kk and were ready to give only 1kk.
3. No one bought access to them, but was broken by a zero.
4. I upload all their 300GB information in archives to the torrent tracker, soon I will distribute it privately in tox to everyone who wants it, and then I will post the links publicly.
5. The function of randomization of links in the notes of the locker has already been implemented, each build of the locker will have a unique link that the dudoser will not be able to recognize.
6. A system of bulletproof storage of data of all companies in the clearnet is being developed, in addition to the torus.
7. I am looking for dudosers in the team, most likely now we will attack targets and provide triple extortion, encryption + date leak + dudos, because I have felt the power of dudos and how it invigorates and makes life more interesting.

Entrust, thanks for the motivation, you make us stronger, and you, as you were a leaky and greedy office, will remain, in a couple of days the whole world will know all your secrets, if I were you, I would pay before it's too late and destroy your information, because for now no one could download it thanks to dudos.

Please do not encrypt correspondence, I do not save the keys.

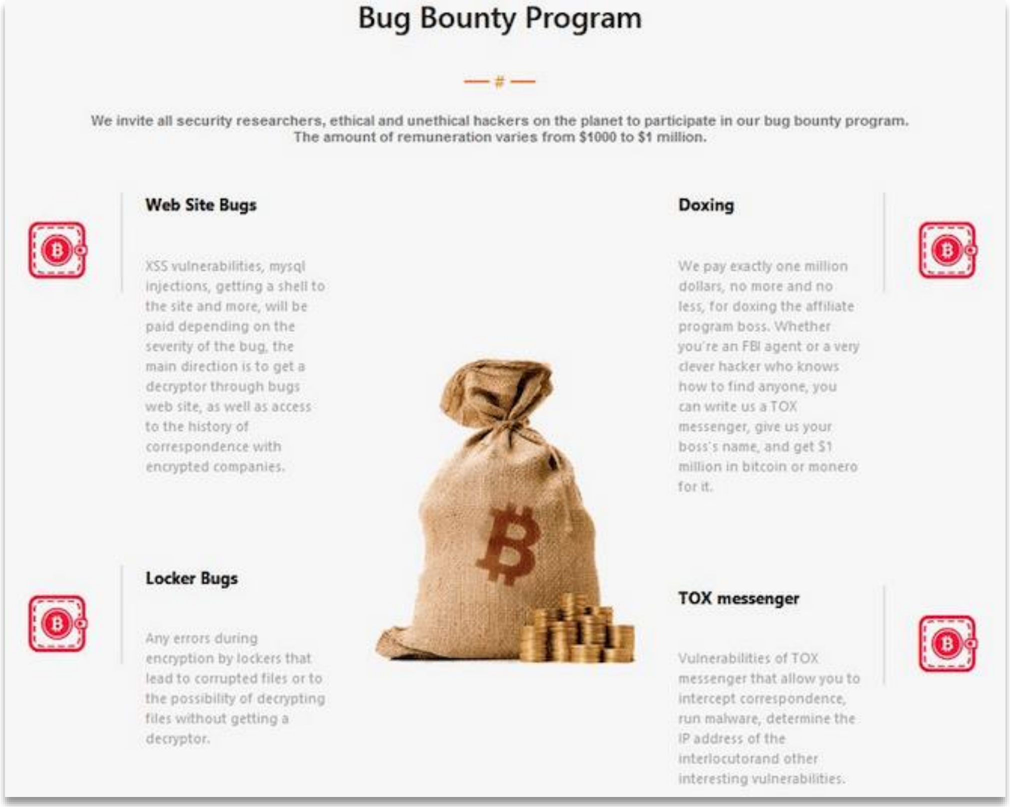
Triple Extortion

Leak Sensitive Data

Demand Ransom

DDoS the Victim

Introduced Bug Bounty



Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program.
The amount of remuneration varies from $1000 to $1 million.

Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.

Locker Bugs

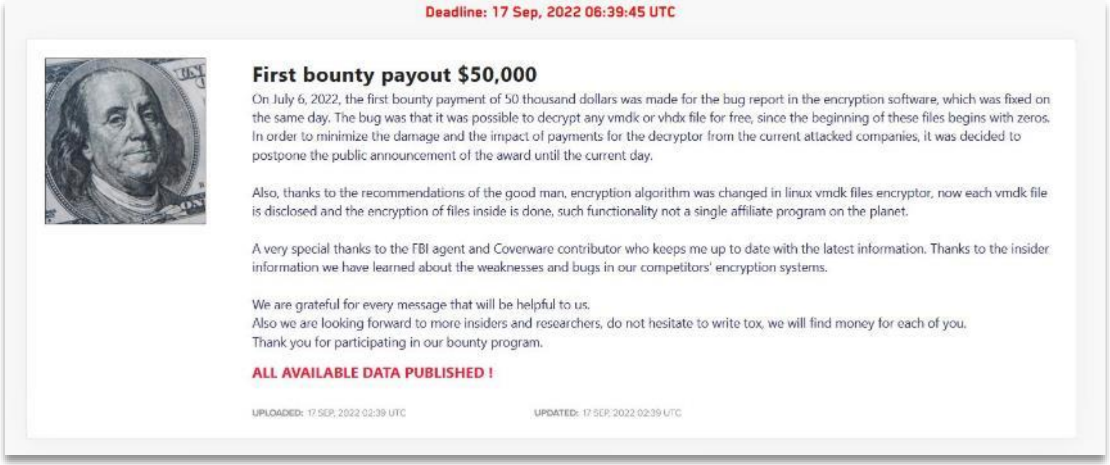
Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decryptor.

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

TOX messenger

Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutorand other interesting vulnerabilities.



Deadline: 17 Sep, 2022 06:39:45 UTC

First bounty payout $50,000

On July 6, 2022, the first bounty payment of 50 thousand dollars was made for the bug report in the encryption software, which was fixed on the same day. The bug was that it was possible to decrypt any vmdk or vhdx file for free, since the beginning of these files begins with zeros. In order to minimize the damage and the impact of payments for the decryptor from the current attacked companies, it was decided to postpone the public announcement of the award until the current day.

Also, thanks to the recommendations of the good man, encryption algorithm was changed in linux vmdk files encryptor, now each vmdk file is disclosed and the encryption of files inside is done, such functionality not a single affiliate program on the planet.

A very special thanks to the FBI agent and Coverware contributor who keeps me up to date with the latest information. Thanks to the insider information we have learned about the weaknesses and bugs in our competitors' encryption systems.

We are grateful for every message that will be helpful to us.
Also we are looking forward to more insiders and researchers, do not hesitate to write tox, we will find money for each of you.
Thank you for participating in our bounty program.

ALL AVAILABLE DATA PUBLISHED !

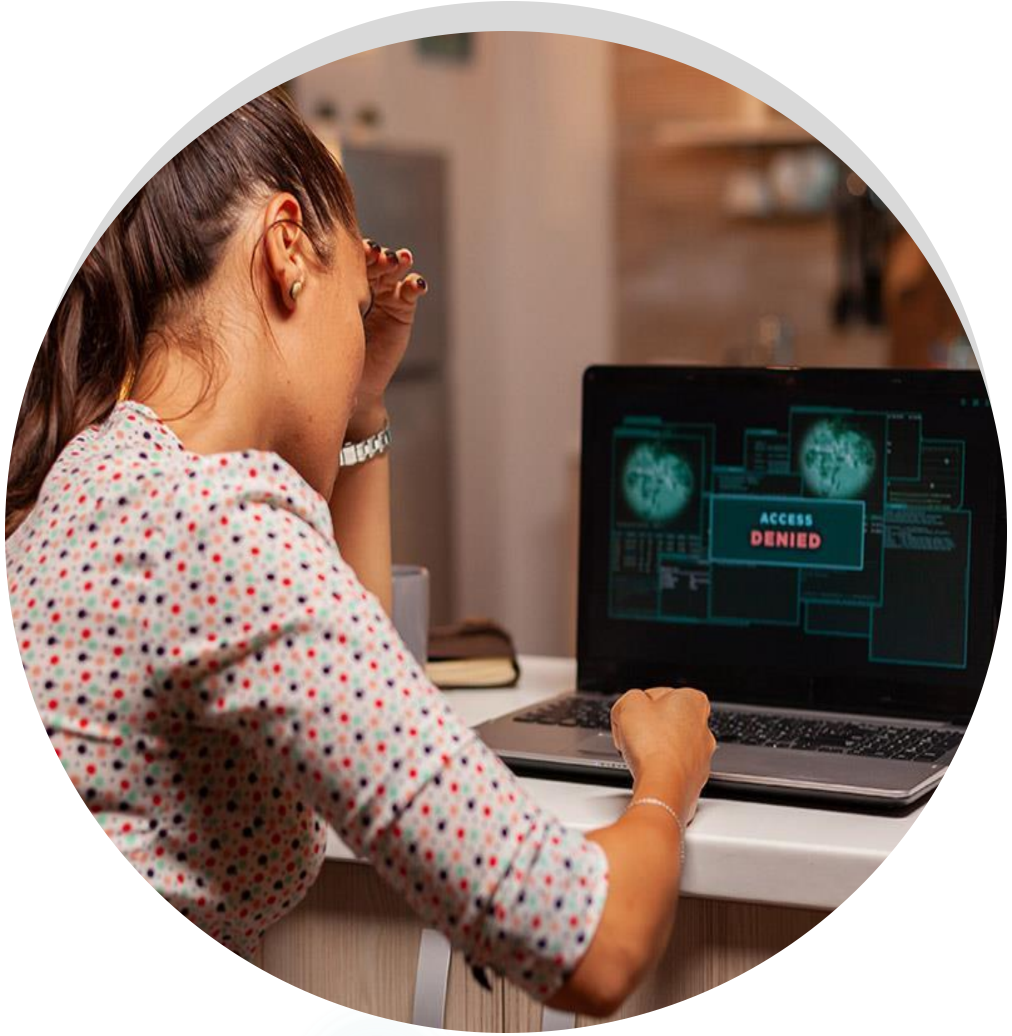
UPLOADED: 17 SEP, 2022 02:39 UTC UPDATED: 17 SEP, 2022 02:39 UTC

Extortion Model

Download Data

Extend Timer

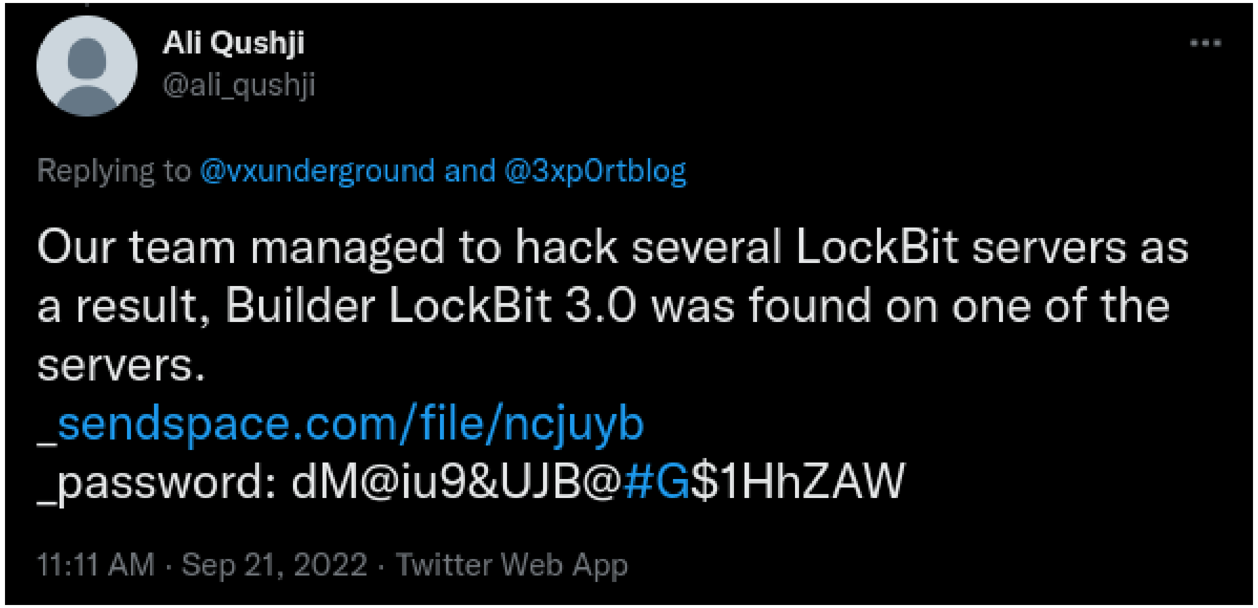
Destroy Data



Conclusion

- Continued targeting of OT industry

- LockBit Black's builder Leak



Ali Qushji
@ali_qushji

Replying to @vxunderground and @3xp0rtblog

Our team managed to hack several LockBit servers as a result, Builder LockBit 3.0 was found on one of the servers.
_sendspace.com/file/ncjuyb
_password: dM@iu9&UJB@#G$1HhZAW

11:11 AM · Sep 21, 2022 · Twitter Web App

OT Protection

- Remediate Bugs
- Update AV
- Implement MFA
- Audit Access
- Observe Enumeration
- Limit Open Ports
- Secure VPN
- Data Backup

Quick Heal

Thank You

Quick Heal Technologies Limited | www.quickheal.co.in | marketing@quickheal.com