EternalRocks (a.k.a. MicroBotMassiveNet)

github.com/stamparm/EternalRocks

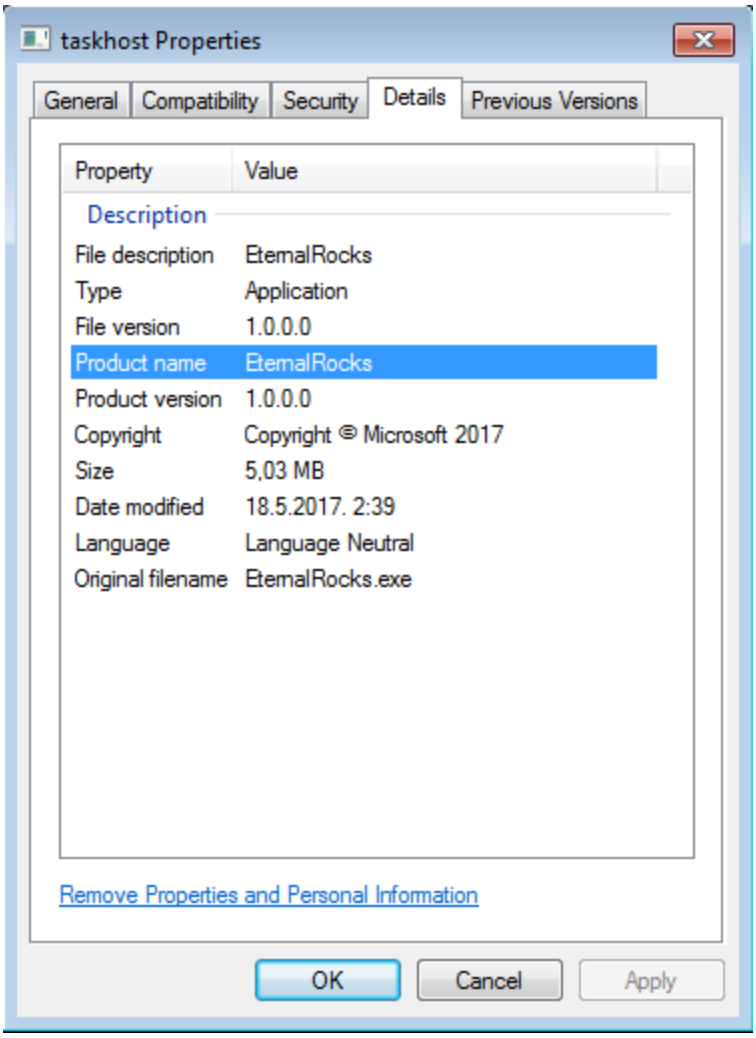
stamparm

stamparm/
EternalRocks

EternalRocks worm

2 Contributors | 1 Issue | 425 Stars | 159 Forks

EternalRocks is a network worm (i.e. self-replicating), emerged in first half of May 2017, with oldest known sample `fc75410aa8f76154f5ae8fe035b9a13c76f6e132077346101a0d673ed9f3a0dd` dating to 2017-05-03. It spreads through public (The Shadow Brokers NSA dump) SMB exploits: `ETERNALBLUE`, `ETERNALCHAMPION`, `ETERNALROMANCE` and `ETERNALSYNERGY`, along with related programs: `DOUBLEPULSAR`, `ARCHITOUCH` and `SMBTOUCH`.

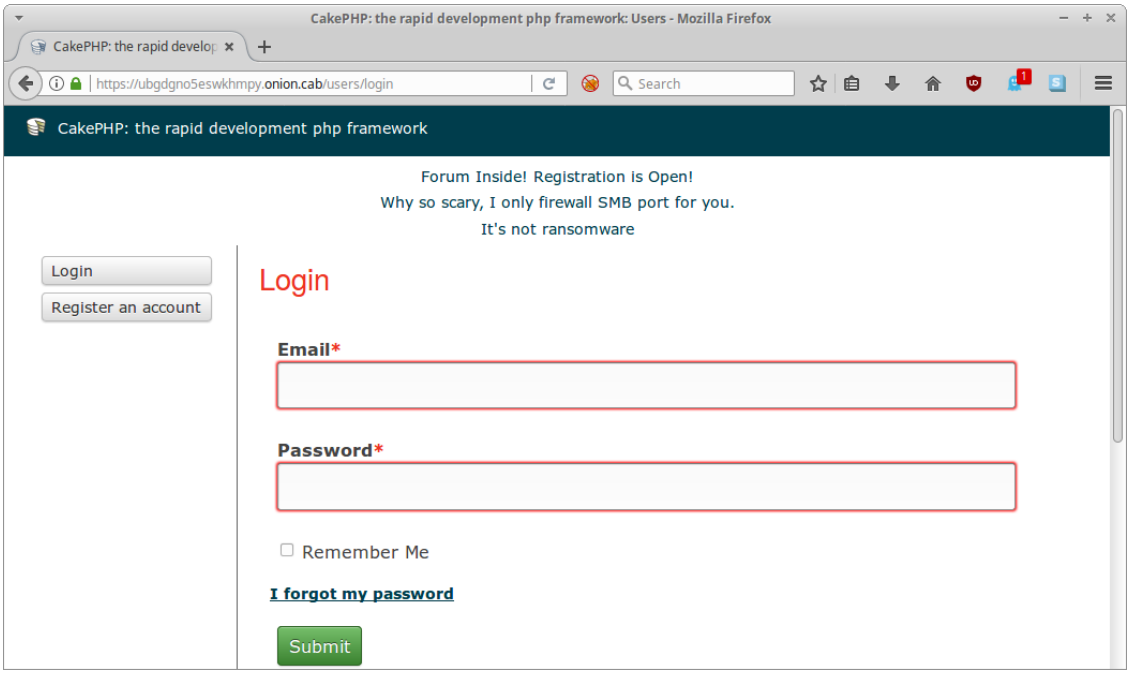


First stage malware `UpdateInstaller.exe` (got through remote exploitation with second stage malware) downloads necessary .NET components (for later stages) TaskScheduler and SharpZLib from Internet, while dropping `svchost.exe` (e.g. sample) and `taskhost.exe` (e.g. sample). Component `svchost.exe` is used for downloading, unpacking and running Tor from `archive.torproject.org` along with C&C (`ubgdgno5eswkhmpy.onion`) communication requesting further instructions (e.g. installation of new components).

Second stage malware `taskhost.exe` (Note: different than one from first stage) (e.g. sample) is being downloaded after a predefined period (24h) from `http://ubgdgno5eswkhmpy.onion/updates/download?id=PC` and run. After initial run it drops the exploit pack shadowbrokers.zip and unpacks contained directories `payloads/` , `configs/` and `bins/` . After that, starts a random scan of opened 445 (SMB) ports on Internet, while running contained exploits (inside directory `bins/`) and pushing the first stage malware through payloads (inside directory `payloads/`). Also, it expects running Tor process from first stage to get further instructions from C&C.

Update (2017-05-25)

Author (" `tmc` ") suddenly drops the whole campaign after a recent fuzz. C&C page currently holds this moment the following (new) message:



After a successful registration, user can find following messages from malware author (" `tmc` ") himself:

```
Its not ransomware, its not dangerous, it just firewalls
the smb port and moves on. I wanted to play some games with
them, considering I had visitors, but the news has to much
about weaponized doomsday worm eternal rocks payload. much
thought to be had... ps: nsa exploits were fun, thanks
shadowbrokers!
```

Message	Its not ransomware, its not dangerous, it just firewalls the smb port and moves on. I wanted to play some games with them, considering I had visitors, but the news has to much about weaponized doomsday worm eternal rocks payload. much thought to be had... ps: nsa exploits were fun, thanks shadowbrokers!
Tstamp	2017-05-24 00:48:00

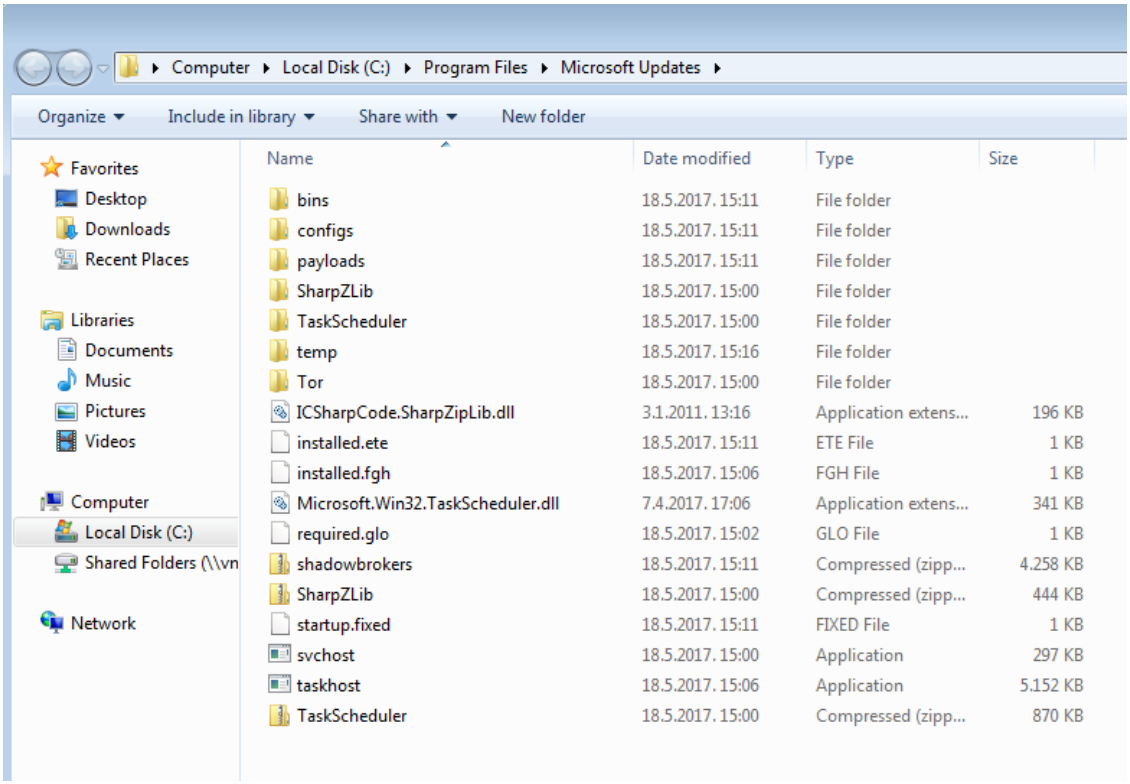
```
btw, all I did, was use the NSA tools for what they were
built, I was figuring out how they work, and next thing I
knew I had access, so what to do then, I was ehh, I will
just firewall the port, thank you for playing, have a nice
a day.
```

Message	btw, all I did, was use the NSA tools for what they were built, I was figuring out how they work, and next thing I knew I had access, so what to do then, I was ehh, I will just firewall the port, thank you for playing, have a nice a day.
Tstamp	2017-05-24 13:33:00

Also, malware doesn't update any more to the (shadowbrokers exploit pack) second stage, but to the dummy executable:

```
// nohost.exe.Program
private static void Main(string[] args)
{
}
```

Host Based indicators



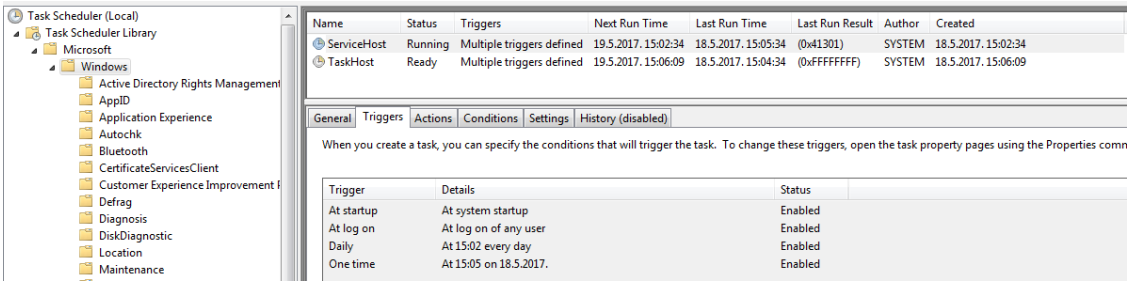
Paths

- `c:\Program Files\Microsoft Updates\SharpZLib.zip` `# in newer variants`
- `c:\Program Files\Microsoft Updates\svchost.exe`
- `c:\Program Files\Microsoft Updates\installed.fgh`

- `c:\Program Files\Microsoft Updates\ICSharpCode.SharpZipLib.dll` `# in newer variants`
- `c:\Program Files\Microsoft Updates\Microsoft.Win32.TaskScheduler.dll`
- `c:\Program Files\Microsoft Updates\SharpZLib\` `# in newer variants`
- `c:\Program Files\Microsoft Updates\temp\tor.zip`
- `c:\Program Files\Microsoft Updates\temp\Tor\`
- `c:\Program Files\Microsoft Updates\required.glo`
- `c:\Program Files\Microsoft Updates\taskhost.exe`
- `c:\Program Files\Microsoft Updates\TaskScheduler.zip`
- `c:\Program Files\Microsoft Updates\TaskScheduler\`
- `c:\Program Files\Microsoft Updates\torunzip.exe` `# in older variants`

Persistence

> Two scheduled tasks `ServiceHost` and `TaskHost` having multiple triggers



Mutexes

- `{8F6F00C4-B901-45fd-08CF-72FDEFF}`
- `{8F6F0AC4-B9A1-45fd-A8CF-72FDEFF}`
- `20b70e57-1c2e-4de9-99e5-69f369006912`

Samples

First stage

- e049d8f69ddee0c2d360c27b98fa9e61b7202bb0d3884dd3ca63f8aa288422dc `# UpdateInstaller.exe (captured)`
- 1ee894c0b91f3b2f836288c22ebeab44798f222f17c255f557af2260b8c6a32d `# UpdateInstaller.exe (variant)`
- 64442cceb7d618e70c62d461cfaafdb8e653b8d98ac4765a6b3d8fd1ea3bce15 `# UpdateInstaller.exe (variant)`
- 94189147ba9749fd0f184fe94b345b7385348361480360a59f12adf477f61c97 `# UpdateInstaller.exe (variant)`
- 9bd32162e0a50f8661fd19e3b26ff65868ab5ea636916bd54c244b0148bd9c1b `# UpdateInstaller.exe (variant)`
- a7c387b4929f51e38706d8b0f8641e032253b07bc2869a450dfa3df5663d7392 `# UpdateInstaller.exe (variant)`
- ad8965e531424cb34120bf0c1b4b98d4ab769bed534d9a36583364e9572332fa `# UpdateInstaller.exe (variant)`
- b2ca4093b2e0271cb7a3230118843fccc094e0160a0968994ed9f10c8702d867 `# UpdateInstaller.exe (variant)`
- c999bf5da5ea3960408d3cba154f965d3436b497ac9d4959b412bfcd956c8491 `# UpdateInstaller.exe (variant)`
- d43c10a2c983049d4a32487ab1e8fe7727646052228554e0112f6651f4833d2c `# UpdateInstaller.exe (variant)`
- d86af736644e20e62807f03c49f4d0ad7de9cbd0723049f34ec79f8c7308fdd5 `# UpdateInstaller.exe (variant)`
- fc75410aa8f76154f5ae8fe035b9a13c76f6e132077346101a0d673ed9f3a0dd `# UpdateInstaller.exe (variant)`

Second stage

- cf8533849ee5e82023ad7adbdbd6543cb6db596c53048b1a0c00b3643a72db30 `# taskhost.exe (captured)`
- 3b4497c7f8c89bf22c984854ac7603573a53b95ed147e80c0f19e549e2b65693 `# taskhost.exe (variant)`
- a77c61e86bc69fdc909560bb7a0fa1dd61ee6c86afceb9ea17462a97e7114ab0 `# taskhost.exe (variant)`
- 70ec0e2b6f9ff88b54618a5f7fbd55b383cf62f8e7c3795c25e2f613bfddf45d `# shadowbrokers.zip (exploits)`

Network indicators

C&C server(s)

`ubgdgno5eswkhmpy.onion`

Downloading required .NET components (first stage)

- `http://api.nuget.org/packages/taskscheduler.2.5.23.nupkg`
- `http://api.nuget.org/packages/sharpziplib.0.86.0.nupkg # in newer variants`

Appendix

Decompilation of an older sample

C# source `# 1ee894c0b91f3b2f836288c22ebeab44798f222f17c255f557af2260b8c6a32d`

```
public class Globals
{
    public static double myVersion = 1.27;

    public static double dVersion = 1.0;

    public static string sInstallDirectory = "C:\\Program Files\\Microsoft Updates";

    public static string sOnion = "http://ubgdgno5eswkhmpy.onion";
}
```

Network traffic capture (PCAP)

Windows 7 x64 SP1 Honeypot `# initial exploitation capture (2017-05-17)`

Yara rules

EternalRocks.yara

Debug strings

- `C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB`
- `C:\Users\tmc\Documents\DownLoader\Project1.vbp`

- `C:\Users\tmc\Documents\TorUnzip\Project1.vbp`
- `c:\Users\tmc\Documents\Visual Studio 2015\Projects\MicroBotMassiveNet\taskhost\obj\x86\Debug\taskhost.pdb`
- `C:\Users\tmc\Documents\Visual Studio 2015\Projects\WindowsServices\svchost\bin\svchost.pdb`

Indicators of Compromise (IOC)

SHA256

```
1ee894c0b91f3b2f836288c22ebeab44798f222f17c255f557af2260b8c6a32d
20240431d6eb6816453651b58b37f53950fcc3f0929813806525c5fd97cdc0e1
2094d105ec70aa98866a83b38a22614cff906b2cf0a08970ed59887383ee7b70
23eeb35780faf868a7b17b8e8da364d71bae0e46c1ababddddddecbdbd2c2c64
3b4497c7f8c89bf22c984854ac7603573a53b95ed147e80c0f19e549e2b65693
44472436a5b46d19cb34fa0e74924e4efc80dfa2ed491773a2852b03853221a2
48b1024f599c3184a49c0d66c5600385265b9868d0936134185326e2db0ab441
589af04a85dc66ec6b94123142a17cf194decd61f5d79e76183db026010e0d31
64442cceb7d618e70c62d461cfaafdb8e653b8d98ac4765a6b3d8fd1ea3bce15
6bc73659a9f251eef5c4e4e4aa7c05ff95b3df58cde829686ceee8bd845f3442
70ec0e2b6f9ff88b54618a5f7fbd55b383cf62f8e7c3795c25e2f613bfddf45d
7b8674c8f0f7c0963f2c04c35ae880e87d4c8ed836fc651e8c976197468bd98a
94189147ba9749fd0f184fe94b345b7385348361480360a59f12adf477f61c97
9bd32162e0a50f8661fd19e3b26ff65868ab5ea636916bd54c244b0148bd9c1b
a77c61e86bc69fdc909560bb7a0fa1dd61ee6c86afceb9ea17462a97e7114ab0
a7c387b4929f51e38706d8b0f8641e032253b07bc2869a450dfa3df5663d7392
ad8965e531424cb34120bf0c1b4b98d4ab769bed534d9a36583364e9572332fa
aedd0c47daa35f291e670e3feadaed11d9b8fe12c05982f16c909a57bf39ca35
b2ca4093b2e0271cb7a3230118843fccc094e0160a0968994ed9f10c8702d867
c4762489488f797b4b33382c8b1b71c94a42c846f1f28e0e118c83fe032848f0
c999bf5da5ea3960408d3cba154f965d3436b497ac9d4959b412bfcd956c8491
cf8533849ee5e82023ad7adbdbd6543cb6db596c53048b1a0c00b3643a72db30
d43c10a2c983049d4a32487ab1e8fe7727646052228554e0112f6651f4833d2c
d86af736644e20e62807f03c49f4d0ad7de9cbd0723049f34ec79f8c7308fdd5
e049d8f69ddee0c2d360c27b98fa9e61b7202bb0d3884dd3ca63f8aa288422dc
e77306d2e3d656fa04856f658885803243aef204760889ca2c09fbe9ba36581d
f152ed03e4383592ce7dd548c34f73da53fc457ce8f26d165155a331cde643a9
fc75410aa8f76154f5ae8fe035b9a13c76f6e132077346101a0d673ed9f3a0dd
```

Imphash

`8ef751c540fdc6962ddc6799f35a907c` `# older (VB6) variants of UpdateInstaller.exe`

Mutexes

```
{8F6F00C4-B901-45fd-08CF-72FDEFF}
{8F6F0AC4-B9A1-45fd-A8CF-72FDEFF}
{8F6F0AC4-B9A1-45fd-A8CF-727220DE8F}
20b70e57-1c2e-4de9-99e5-69f369006912
```

File paths

```
c:\Program Files\Microsoft Updates\
```

Scheduled tasks

`ServiceHost -> C:\Program Files\Microsoft Updates\svchost.exe # system start, log on, daily`

`TaskHost -> C:\Program Files\Microsoft Updates\taskhost.exe # system start, log on, daily`