Win32/Duqu: involution of Stuxnet

Aleksandr Matrosov

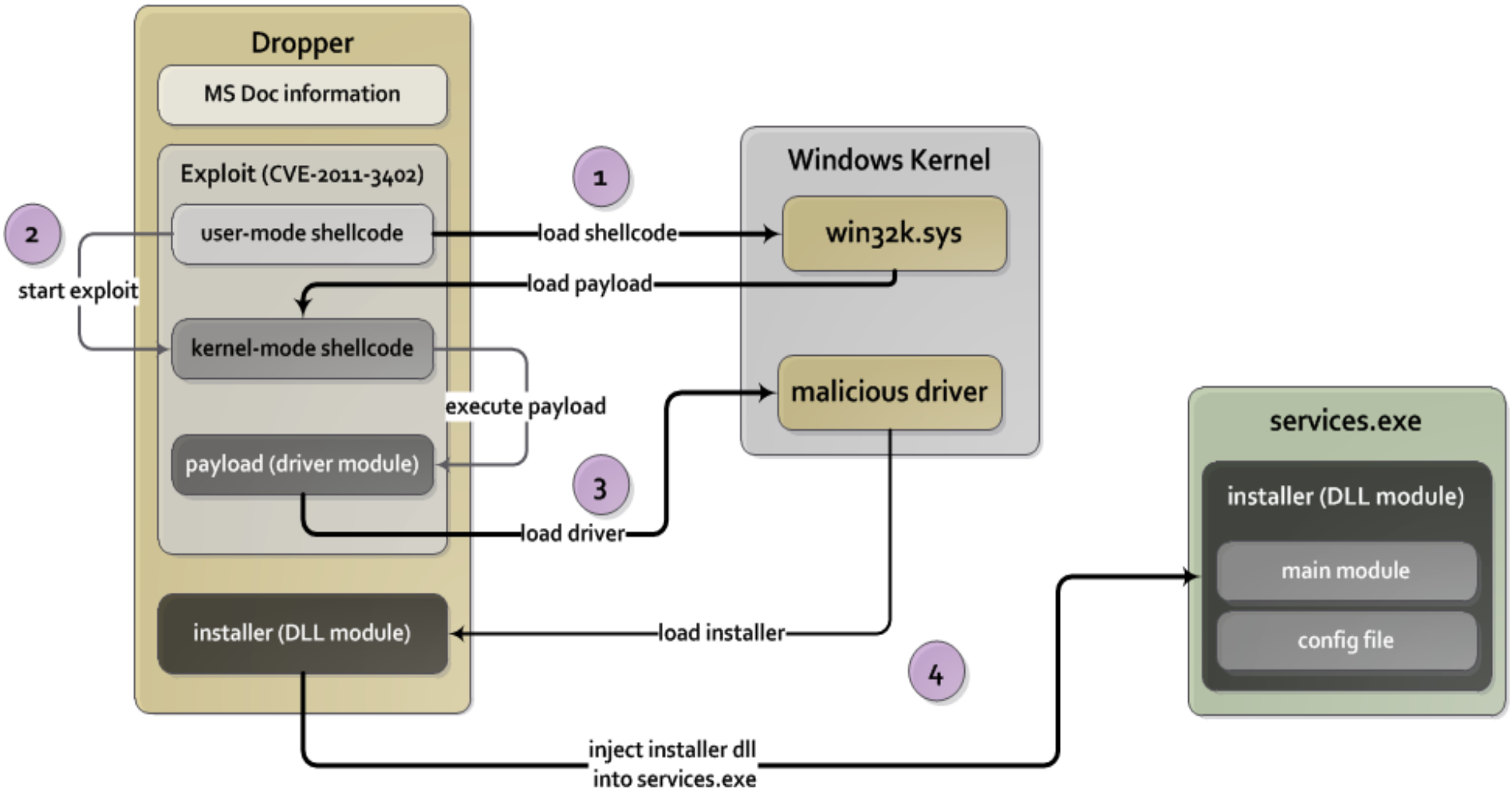
Eugene Rodionov

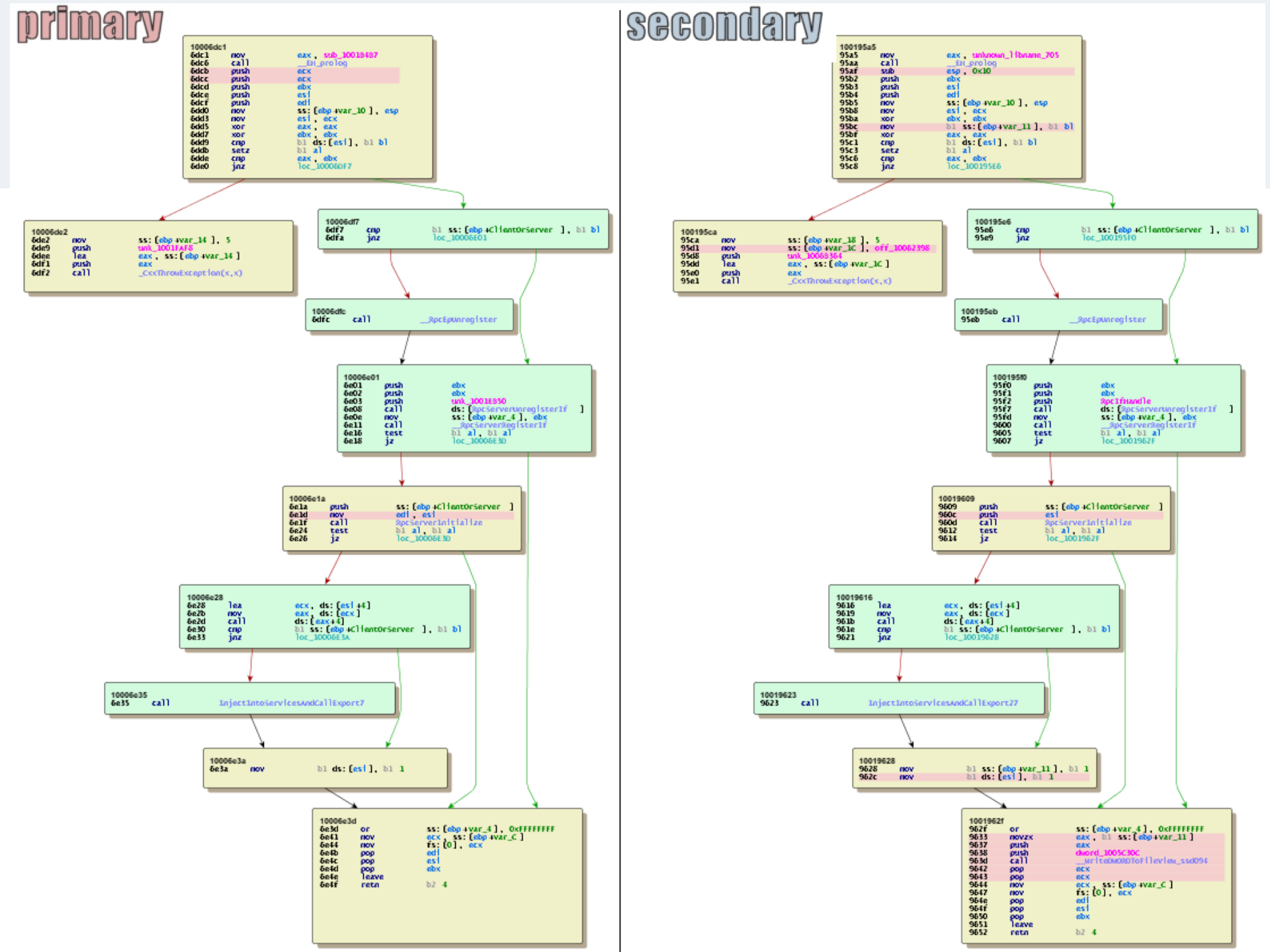
we protect your digital worlds

Инволю́ция (от лат. *involutio* — свёртывание) — редукция или утрата в процессе эволюции отдельных органов, упрощение их организации и функций

14.10	19.10	01.11	03.11	4.11	?
CrySyS Lab share info about Duqu on public	Duqu: the precursor to the next Stuxnet	Dropper found and 0-day confirmed CVE-2011-3402	Microsoft Security Advisory (2639658)	MS share info about exploit on MAPP	What the next?

Duqu infection scheme




primary
secondary

RPC Function	Stuxnet	Duqu
Rpc 1– return version of the worm	☑	☑
Rpc 2 – load module in into a new process and execute export function	☑	☑
Rpc 3 – load module into existing process and execute export #1	☑	☒
Rpc 4 – load module in a process and execute its entry point	☑	☑
Rpc 5 – Build the worm dropper	☑	☒
Rpc 6 – run specified application (calling CreateProcess API)	☑	☑
Rpc 7 – read data from specified file	☑	☑
Rpc 8 – write data into specified file	☑	☑
Rpc 9 – delete specified file	☑	☑
Rpc 10 – work with target files	☑	☒

Finding exact date of infection

```
EnterCfgData(&CfgMutex);
v8 = 0;
bDeleteItself = GetConfigBuffer()->bCheckSelfDelete;
v8 = -1;
result = LeaveCfgData(&CfgMutex);
if ( !bDeleteItself )
{
  EnterCfgData(&_CfgMutex);
  v8 = 1;
  EnterCfgData(&CfgMutex);
  LOBYTE(v8) = 2;
  v3 = GetConfigBuffer();
  v4 = GetConfigBuffer();
  bTimeElapsed = IsTimeElapsed(&v4->InfectionDate, v3->DaysToLive);// check time to remove itself from the system
  LOBYTE(v8) = 1;
  LeaveCfgData(&CfgMutex);
  v8 = -1;
  result = LeaveCfgData(&_CfgMutex);
  if ( bTimeElapsed )
    result = InjectAndExecuteExportFunction(2, 0);// call export 2 (remove itself from the system)
```

Config decryption algorithm

```
def decrypt(data):
    gamma = [0x2b, 0x72, 0x73, 0x34, 0x99, 0x71, 0x98, 0xAE]

    a = 0
    for ix in xrange(len(data)):
        data[ix] ^= gamma[a]
        a = a + 1
        if a == 7:
            a = 0
```

Finding date in UTC format

11/08/2011 at 07:50:01

36

18/08/2011 at 07:29:07

30


PLEASE STAND BY

References

✓“Win32/Duqu: It’s A Date”

http://blog.eset.com/2011/10/25/win32duqu-it’s-a-date

✓“Stuxnet Under the Microscope”

http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

✓“Win32/Duqu analysis: the RPC edition”

http://blog.eset.com/2011/10/28/win32duqu-analysis-the-rpc-edition

✓Follow ESET Threat Blog

http://blog.eset.com

Thank you for your attention ;)

Aleksandr Matrosov
matrosov@eset.sk
@matrosov

Eugene Rodionov
rodionov@eset.sk
@vxradius