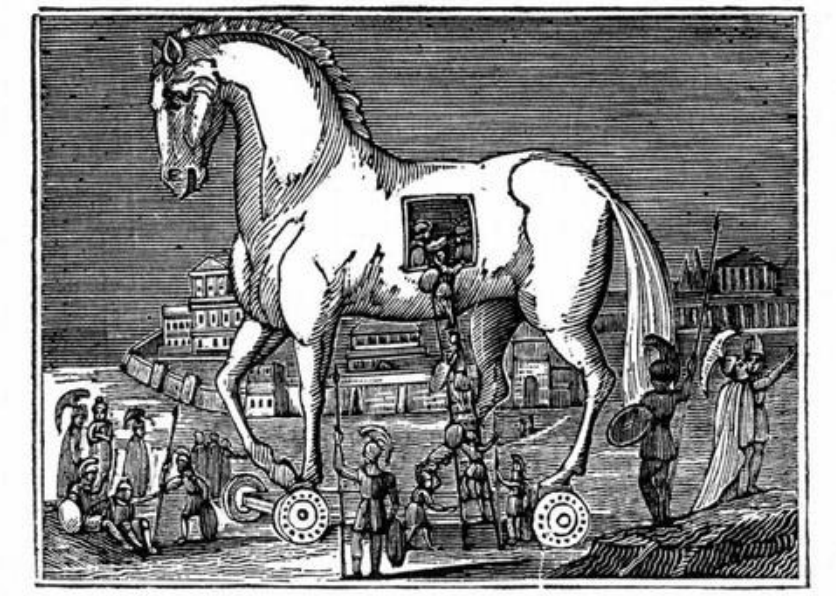
VERAMINE DYNAMIC DECEPTION SYSTEM

Version 1.8.2



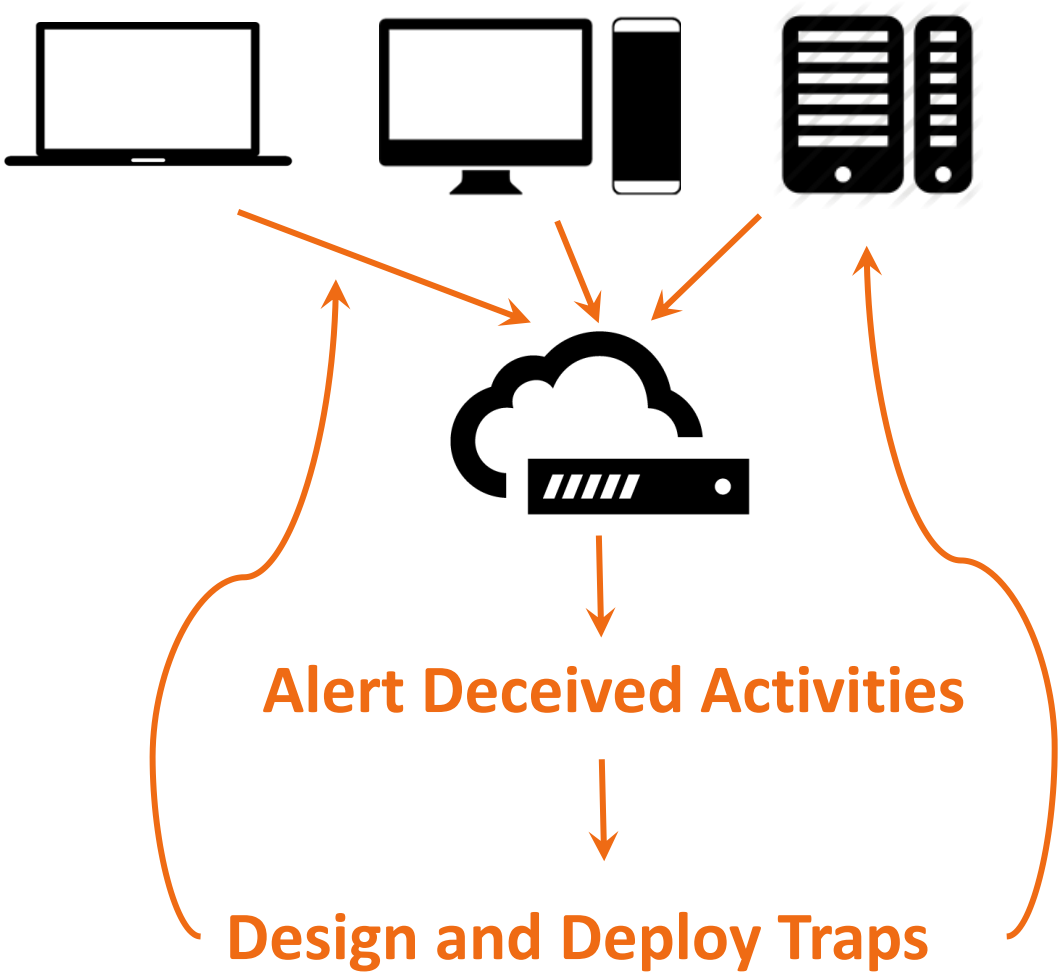
Trojans Deceived.

AUGUST 21, 2019

Mục lục

Deception Introduction

Dynamic Deception System (DDS), a Platform of Security Traps uniquely offered by Veramine, such as Deceptive services, processes, mutexes, credentials, network listeners, data shares, registry helper..., that can be deployed to any set of Hosts, as an Active Defense approach to Detect and Prevent attacks. Most other existing approaches are Passive Defense. VDDS is capable of making every computer (physical or VM) a honeypot, in IT Systems. The traps are put along the kill chain, to cheat, detect and prevent intrusions, track intruders' activities, and limit things they can do.



The Veramine platform provides a set of deception tactics that can be customized and deployed to endpoints. A tactic is a type of deception, i.e., a file, a service, mutex, etc. These files backing these tactics are controlled by Veramine. The supported tactics are:

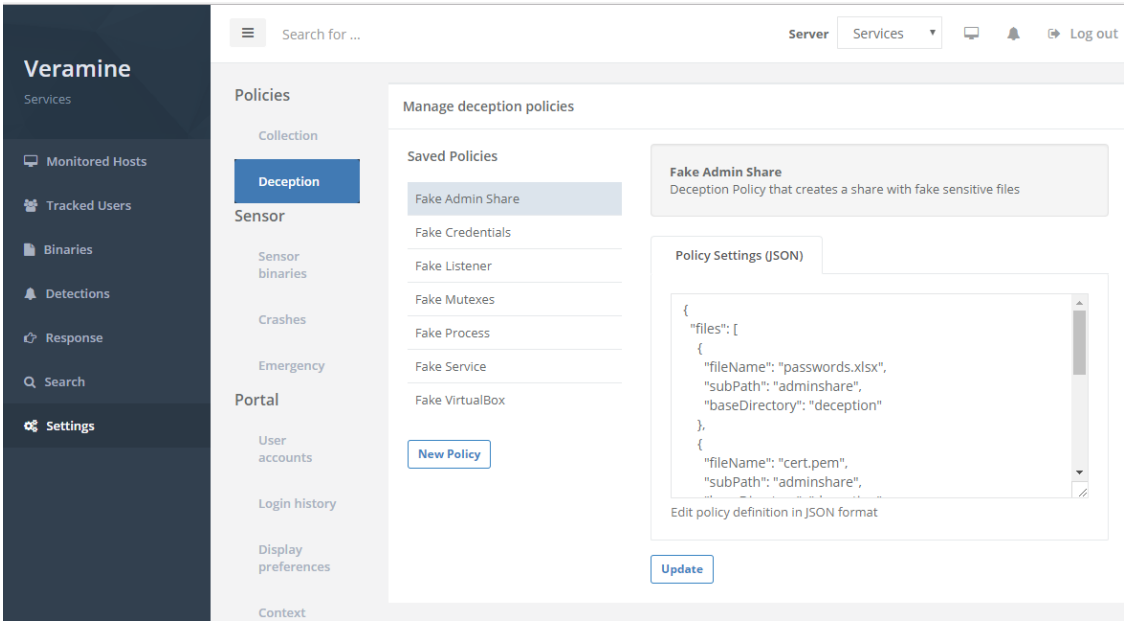
1. Services
2. Processes
3. Files
4. Registry
5. User credentials

6. SMB shares
7. Network listeners
8. Mutexes
9. Events

The parameters for each tactic are described in a later section.

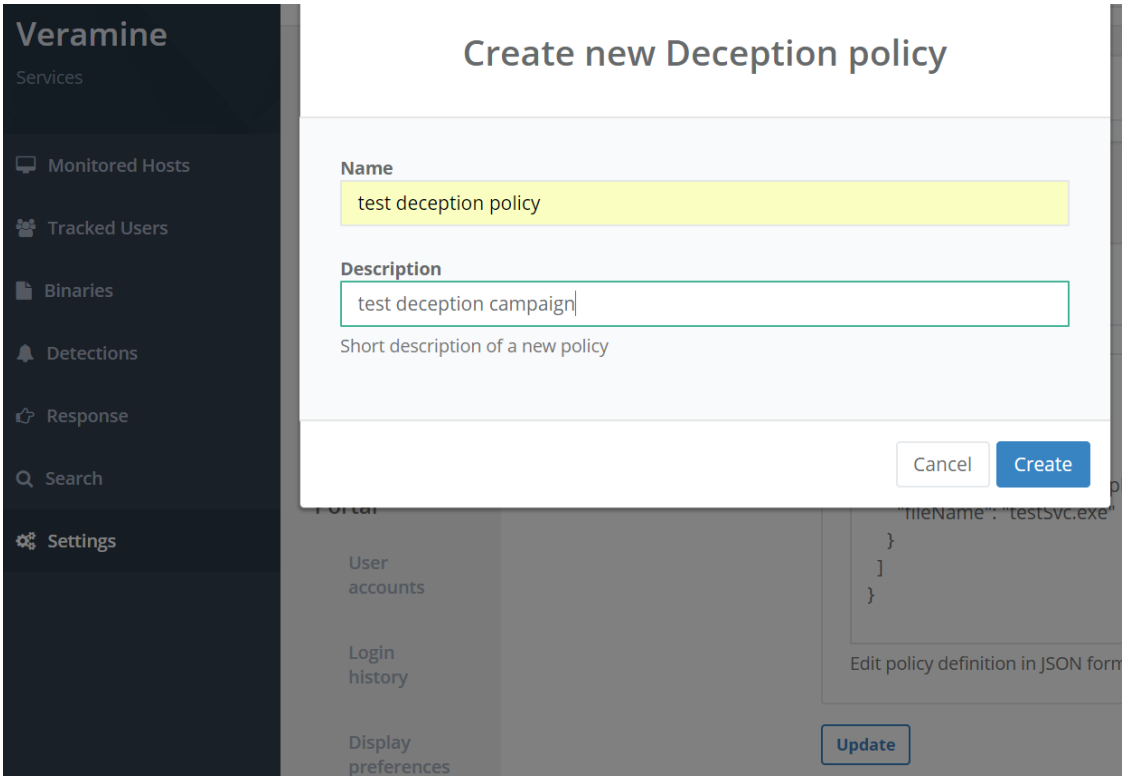
Deployment procedures

Tactics are listed and updated using JSON via the portal (Settings, Policies, Deception):



Deception policy setting

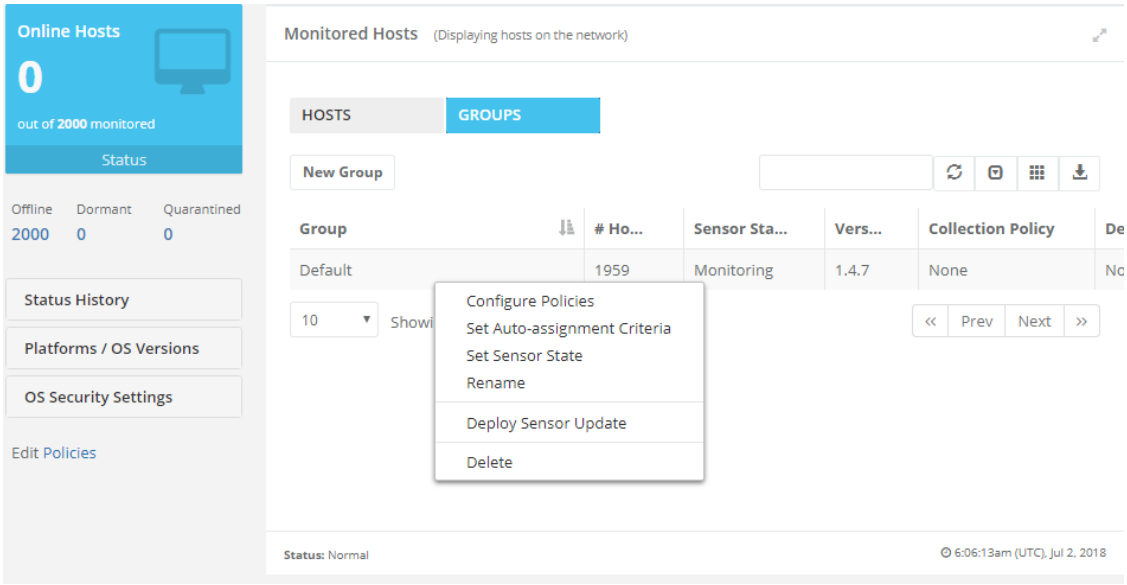
There are pre-made deception tactics which can be deployed immediately. If you want to create a new deception tactic, click “New Policy” to create a new deception policy; fill in the information as requested and click “Create”,



Deception policy box

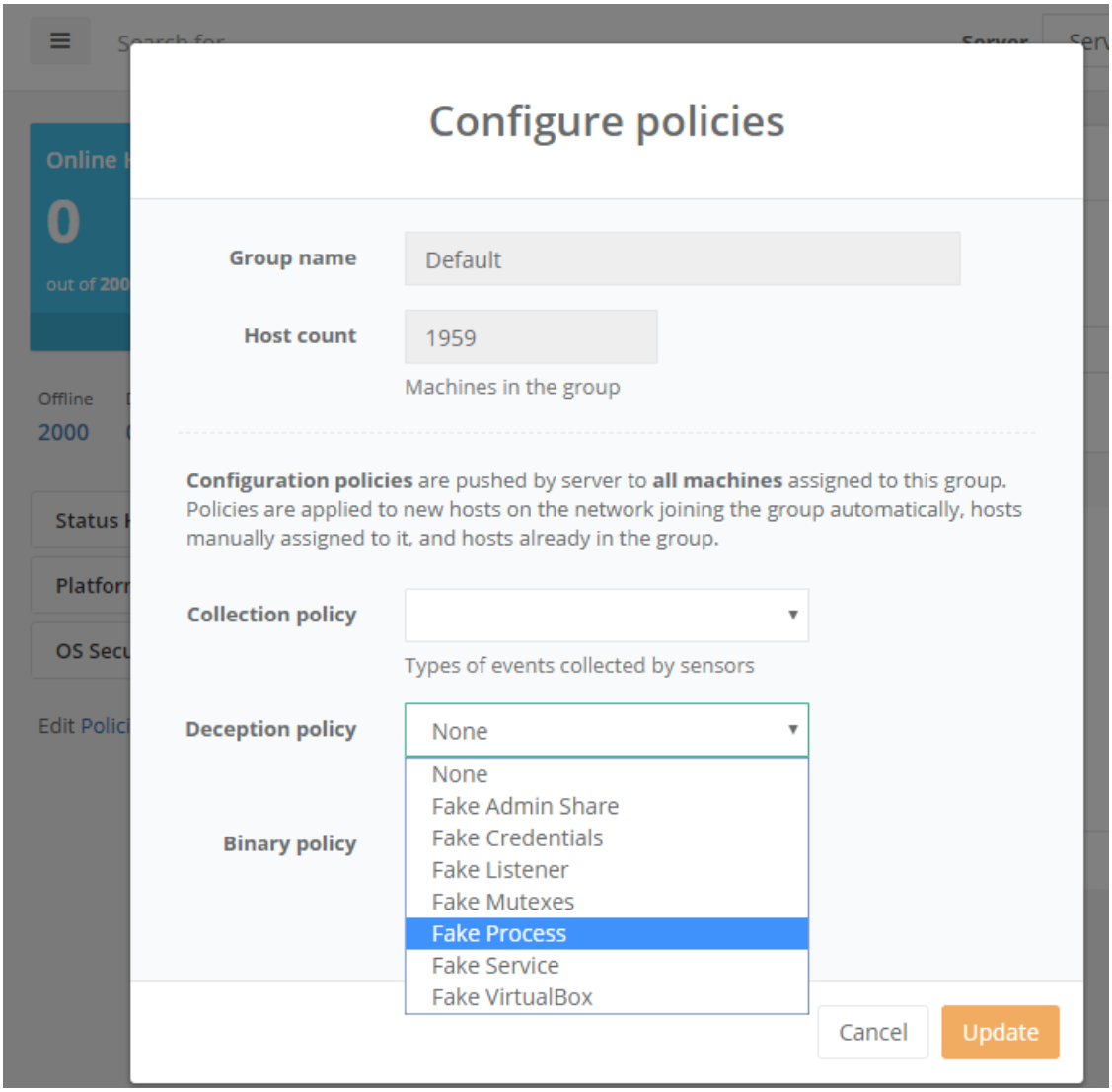
Policies can also be updated by changing the JSON and clicking “Update” at the bottom right.

To deploy a tactic, go to the “Groups” view, right click on the group and select “Configure Policies”,



Configure policies for a group

Then you can pick the deception policy from the list and click “Update.”



Deploying policies to a group

To uninstall a policy, simply change it to “None” and click update.

Tactic description and parameters

The following section describes each tactic and its parameters.

Services

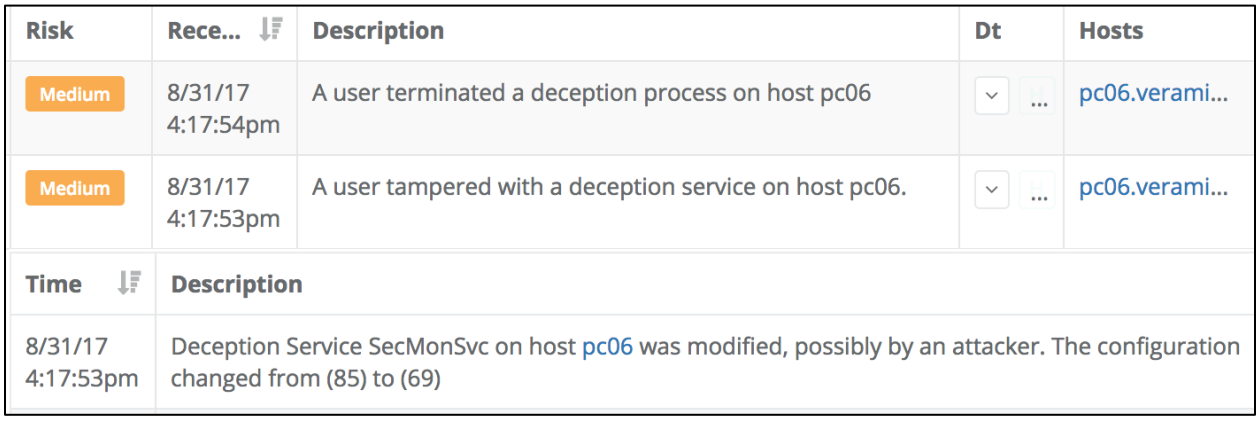
You can deploy a service with a specified filename on the remote system. The parameters are:

- `name`: the service’s name (i.e., the parameter to `sc stop/start`). It cannot have spaces.
- `displayName`: the service’s long description.
- `filename`: the name to be used for the service executable.

Here is a JSON describing two services,

```
{
  "services": [
    {
      "name": "testSvc",
      "displayName": "test display name",
      "fileName": "testSvc.exe"
    },
    {
      "name": "testSvc2",
      "displayName": "test2 display name",
      "fileName": "testSvc2.exe"
    }
  ]
}
```

Example of a deceptive service is tampered with:



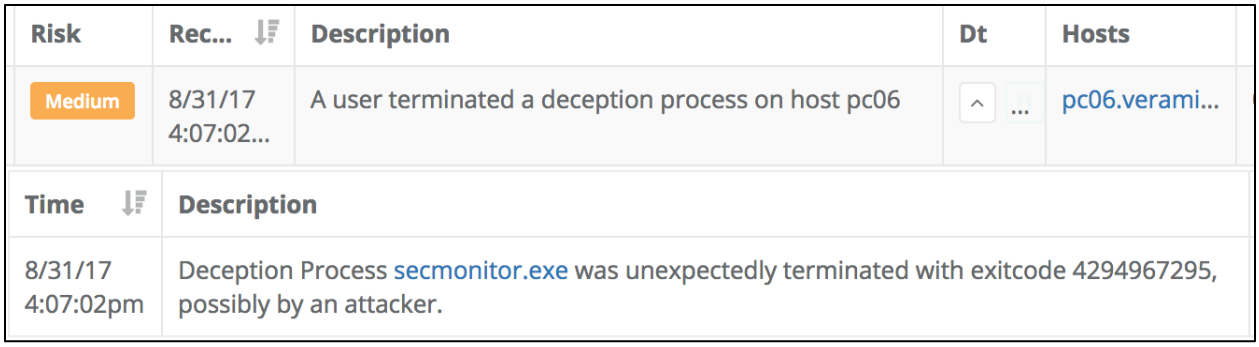
Processes

You can specify a process with a certain name to be launched. The parameters are:

```
{
  "processes": [
    {
      "fileName":"process.exe",
      "baseDirectory": "ProgramFiles"
    }
  ]
}
```

The valid base directories include the following: `ProgramFiles`, `ProgramFilesX86`, `Windows`, `System32`, `Drivers`, `Deception`.

Example of a deceptive process is terminated:



Files

Files can be placed in specific directories. The parameters are:

- `fileName`: the file name. The content of the file is provided by Veramine.
- `baseDirectory`: the base directory in which to write the file.

Example:

```
{
  "files": [
    {
      "fileName": "test1.exe",
  "baseDirectory": "Windows"
    },
    {
      "fileName": "test2.exe",
  "baseDirectory": "Windows"
    }
  ]
}
```

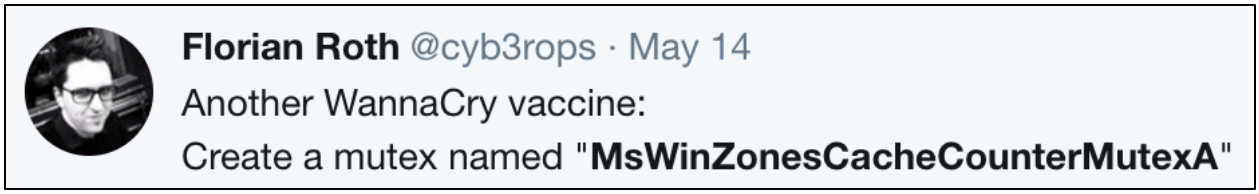
Mutexes

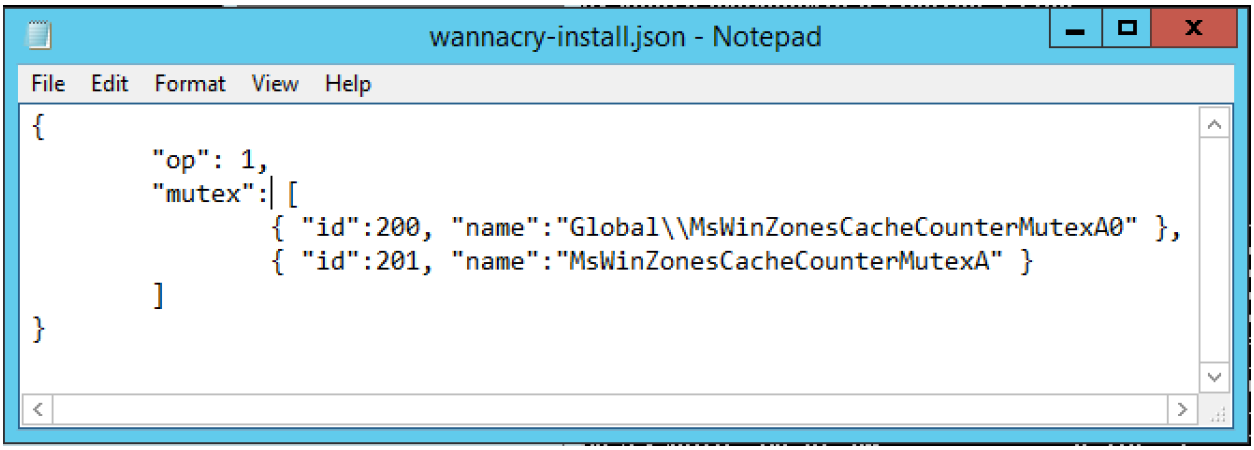
You can create a mutex. The parameters are:

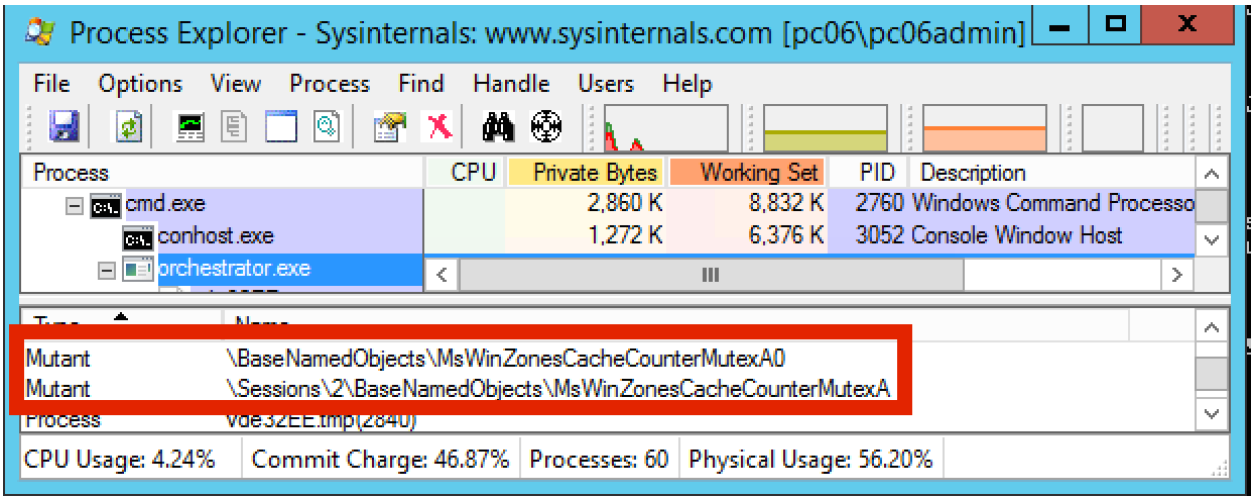
- `name`: the name of the mutex. If you want it to be global, it needs to be prefixed with "Global\".

```
{
  "mutexes": [
    {
      "name": "Global\\crazyMutex"
    }
  ]
}
```

Example, WannaCry checks a mutex to decide if a system is already infected. We can set such a deceptive mutex.







Events

You can create an event. The parameters are:

- `name`: the name of the event. If you want it to be global, it needs to be prefixed with “Global\”.

Example:

```
{
  "events": [
    {
      "name": "Global\\crazyEvent"
    }
```

```
  ]
}
```

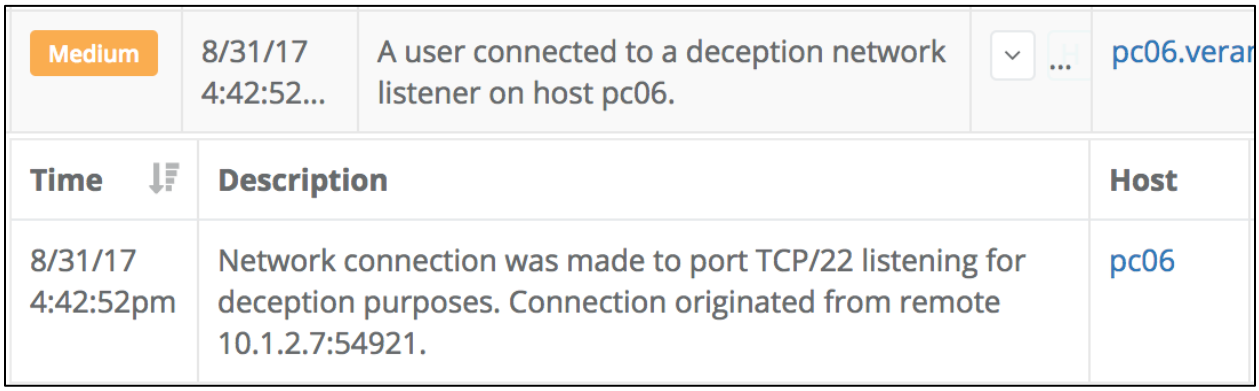
Network listener

A network listener is a process that binds to a TCP port and accepts connections. The parameters are:

- `port`: TCP port to listen on.

Example:

```
{
  "listeners": [
    {
      "port": 31337
    }
  ]
}
```



Credentials

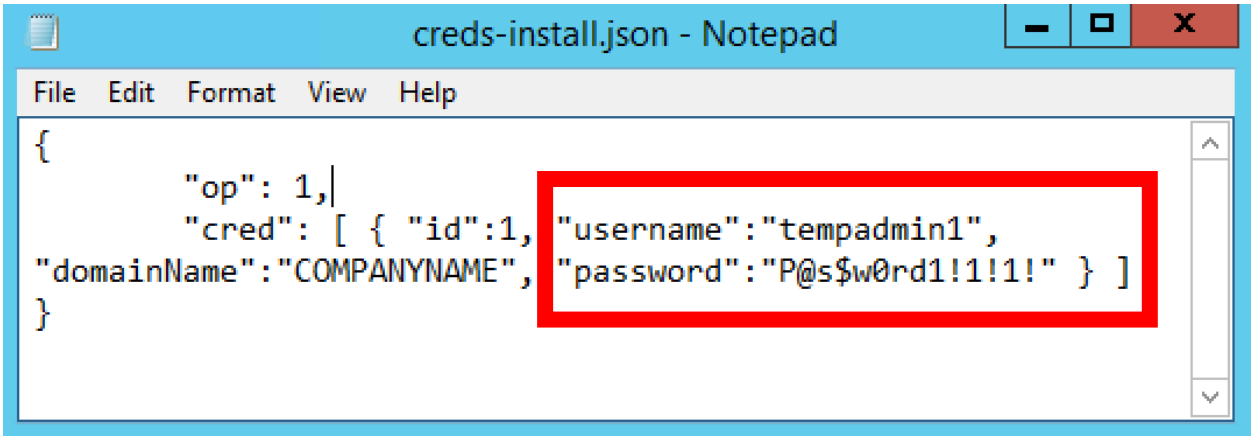
Credentials can be injected to Windows authentication subsystem. Note that these usernames/passwords may be real or fictitious. The parameters are:

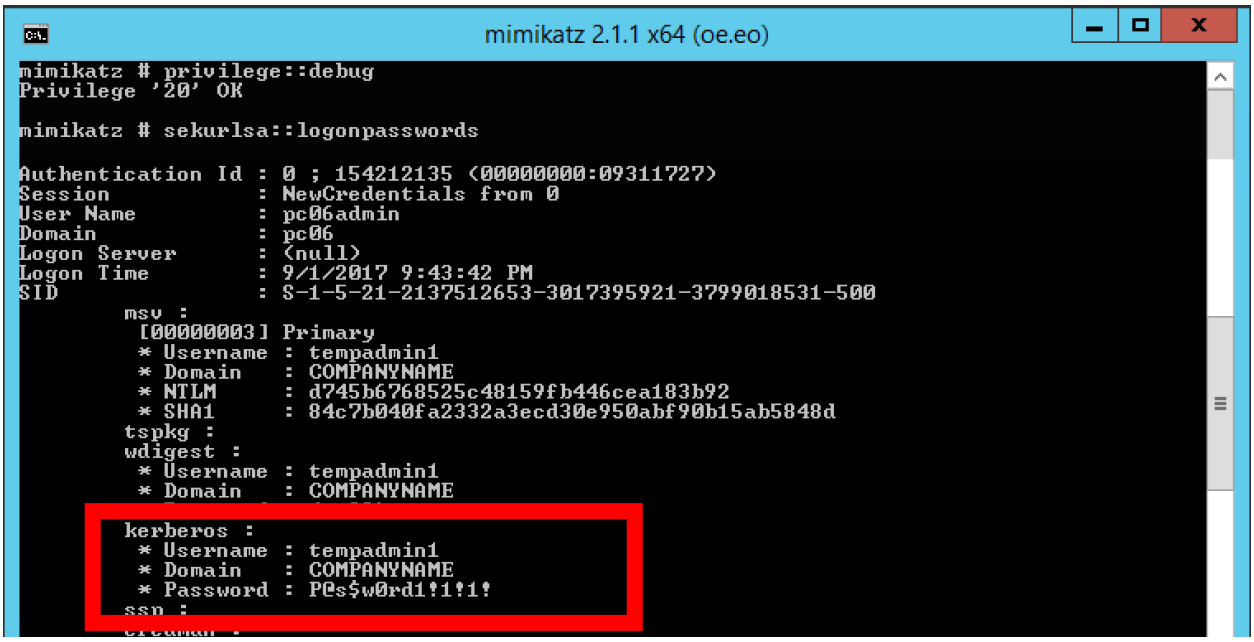
- `domain`: the domain of the user.
- `userName`: username.
- `password`: password.

Example:

```
{
  "credentials": [
    {
      "domain": "exampleDomain",
      "username": "user",
      "password": "myPassword"
    }
```

```
  ]
}
```





Network shares

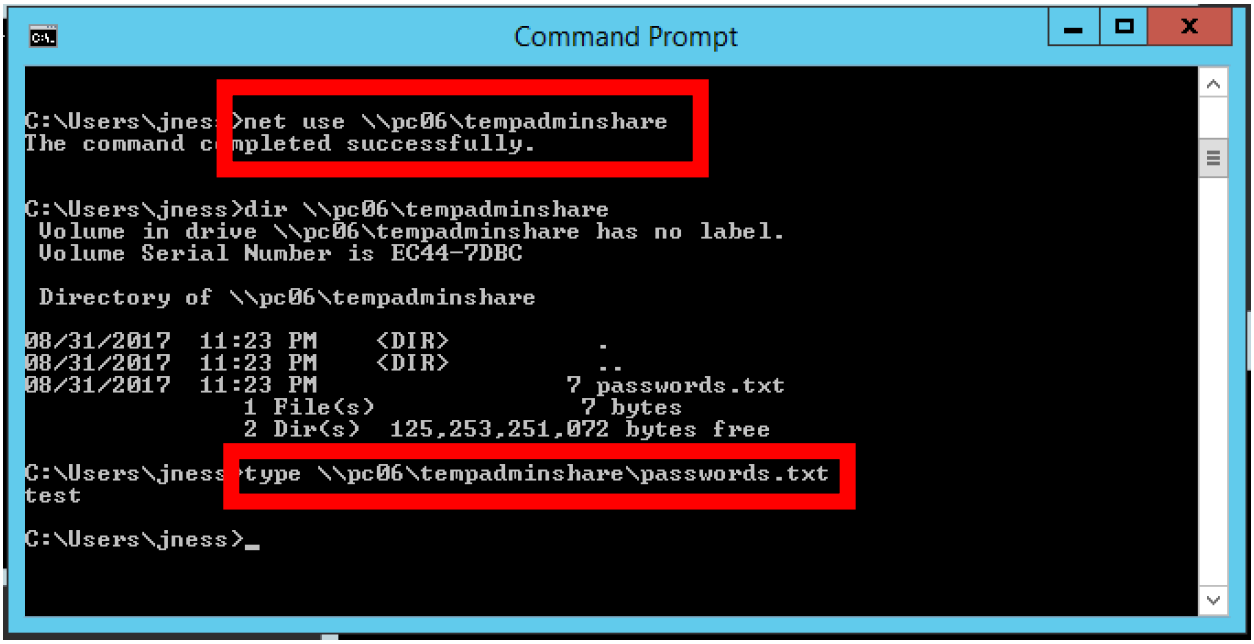
Network shares share a directory to the world. The parameters are:

- `name`: the name of the network share.
- `description`: the description of the network share.

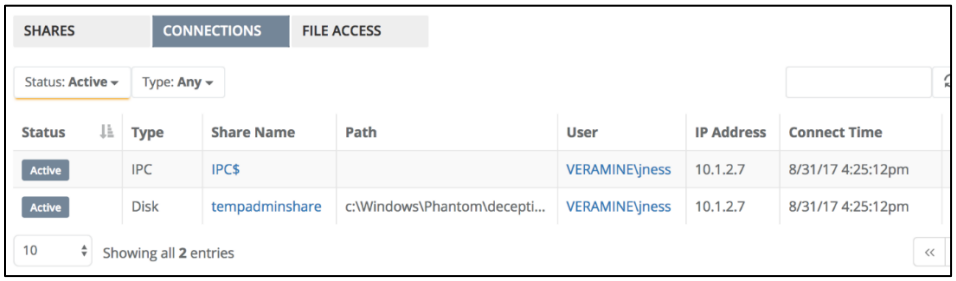
Example:

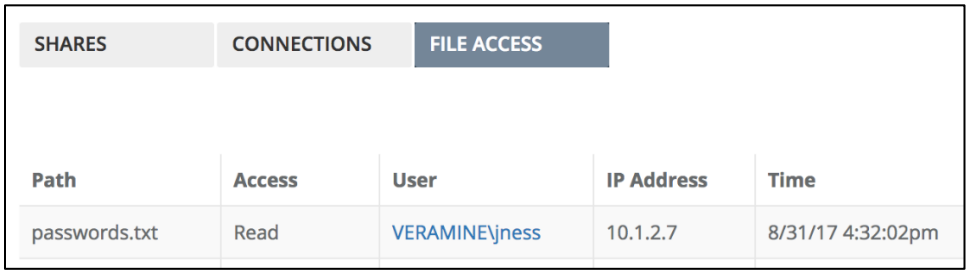
```
{
  "shares": [
    {
      "name": "testShare",
  "description": "Test Share"
    }
```

```
  ]
}
```


Command Prompt
C:\Users\jness>net use \\pc06\tempadminshare
The command completed successfully.
C:\Users\jness>dir \\pc06\tempadminshare
Volume in drive \\pc06\tempadminshare has no label.
Volume Serial Number is EC44-7DBC
Directory of \\pc06\tempadminshare
08/31/2017 11:23 PM <DIR> .
08/31/2017 11:23 PM <DIR> ..
08/31/2017 11:23 PM 7 passwords.txt
1 File(s) 7 bytes
2 Dir(s) 125,253,251,072 bytes free
C:\Users\jness>type \\pc06\tempadminshare\passwords.txt
test
C:\Users\jness>


SHARES
CONNECTIONS
FILE ACCESS
Status: Any
Type: Disk
Status
Type
Share Name
Path
Owner
Create Time
Active
Disk
tempadminshare
c:\Windows\Phantom\deception\share1
BUILTIN\Administrators
8/31/17 4:23:59...
10
Showing all 1 entries


SHARES
CONNECTIONS
FILE ACCESS
Status: Active
Type: Any
Status
Type
Share Name
Path
User
IP Address
Connect Time
Active
IPC
IPC$
VERAMINE\jness
10.1.2.7
8/31/17 4:25:12pm
Active
Disk
tempadminshare
c:\Windows\Phantom\decepti...
VERAMINE\jness
10.1.2.7
8/31/17 4:25:12pm
10
Showing all 2 entries


SHARES
CONNECTIONS
FILE ACCESS
Path
Access
User
IP Address
Time
passwords.txt
Read
VERAMINE\jness
10.1.2.7
8/31/17 4:32:02pm

Risk	Rece...	Description	Dt	Hosts	Inst #
Medium	8/31/17 4:25:12pm	A user established a connection to a deception share on host pc06.		pc06.verami...	1

Time	Description	Host
8/31/17 4:25:12pm	Deception SMB Share tempadminshare on host pc06 was accessed by user VERAMINE\jness from host with IP address(es) 10.1.2.7	pc06

Risk	Rec...	Description	Dt	Hosts
Medium	8/31/17 4:32:02...	A user accessed a file on a deception share on host pc06.		pc06.veran

Time	Description	Host
8/31/17 4:32:02pm	A file named passwords.txt on Deception Share tempadminshare (host pc06) was opened for reading by user VERAMINE\jness from host with IP address(es) 10.1.2.7	pc06

Registry

Registry values can be set matching interesting preconfigured scenarios. The current version sets registry keys to spoof the presence of a virtual machien. The tactic names are:

- `VMWare`: spoof VMWare registry keys.
- `VirtualBox`: spoof VirtualBox registry keys.
- `Qemu`: spoof Qemu registry keys.
- `HyperV`: spoof HyperV registry keys.

Example:

```
{
  "reg": [
    {
      "tactic": "VMWare"
    }
  ]
}
```

Appendix A: Outstanding Features of Veramine Suite

Veramine Inc.

Advanced Endpoint Security

Specialized in building **cybersecurity endpoint** products, awarded contracts worth **multi-million USDs** from

- **U.S. Department of Homeland Security (DHS),** also recommended by DHS as a platform for **financial and banking sector customers**
- **U.S. Department of Defense (DOD)**
- **U.S. Airforce**
- **ANZ**, a **top-3 bank** in Australia
- **And other important customers…**

Products, for **SOC**, **MSSP** or **IT** admins, **On-premise** or **Cloud**
- Veramine Endpoint Detection and Response (**VEDR**)
- Veramine Dynamic Deception System (**VDDS**)
- Veramine Advanced Activities Monitoring (**VAAM**)

Customers' **Compliments**: "unique and powerful capabilities for detailed data collection, monitoring, control, yara memory search, forensics, incident response, and detection"

Data Collection and Advanced Monitoring

***Data Quality**: Wide Variety. Detailed. Structured. Real Time. Small Traffic. All security-related activities, especially System Security and SMB data, is probably only collected by Veramine: **Process, Registry, System Security, Network, User, SMB, Binaries**…*

Flexible collection policies: admins can select what data to collect. **Adaptive filter**: sensors smartly don't send irrelevant high-volume events to servers, that can filter out TB's of traffic sent and processed by sensors and servers.

***External** and **Insider Threats** Prevention with **Advanced Monitoring** on Data, Devices and Users, such as User and Entity Behavior Analytics (UEBA), Key loggers, Screenshot captures, Activities of Browsing-Email-SMB, User sessions, USB Management Logged Tracking and Access Control Policies (**Blocked**, **Read-Only**, or **Read-Write**).*

Detection and Deception

*Aim to detect all **attack tactics and techniques** in https://attack.mitre.org/wiki/Technique_Matrix, the Attack Dictionary.*

More collected data types allow more data analysis algorithms, combining rule-based and machine learning, resulting in **better Detection**. Examples: SMB data allows detecting **Lateral Movement** and **Insider Threat**; Precise Elevation of Privilege (**EOP**) detection by collecting security tokens; Lsass process open allows detecting credentials and passwords dumping (**Mimikatz**); Command arguments allow detecting **Malicious Powershell Fileless** intrusion…

Deception** is an **Active Defense** approach, whereas most existing approaches are Passive Defense. **Platform of Traps**, put along the kill chain, to **cheat, detect and prevent** intrusions**.** Capable of making **every computer** (physical or VM) a **honeypot**, in IT Systems. **Uniquely offered by Veramine.

Deceptive **services, processes, files, mutexes, credentials, network listeners, data shares, registry helper, VMs**… **Track** intruders' activities, and **limit** things they can do, with the traps. E.g. **WannaCry** checks a mutex to decide if a system is already infected. We can set such a deceptive mutex.

Incident Response and Forensics

Yara Search *on Memory and Files is Unique of Veramine.* ***Memory dumps*** *are at fingertips. All collected data is* ***searchable*** *using very* ***flexible logical expressions****. All* ***executable binaries*** *are collected for forensics.*

Veramine have **most Response Actions**, from **Binaries, Users, Hosts** to **Processes**. E.g. Network Quarantine, Process Suspend/Terminate, User Disable/Disconnect, Host Sleep/Shutdown/Restart, Binary Block, Scan with Virus Total…

Forensics *with Velociraptor to collect various* ***built-in*** *or* ***customized artifacts*** *from* ***multiple endpoints*** *in* ***real-time*** *from centralized portal.* ***VQL****, similar to SQL, allows collection tasks to be quickly programmed, automated and shared, so that* ***turn-around*** *from IOC to full hunt can be a few minutes. E.g. VQL to collect files in users' temp directory which have been created within the last week.*

Performance, Deployment, Integration and Management

Veramine sensors on average take less than **1% CPU** and **20 MB RAM**, network traffic is less than **30 MB/day/host**, and can be further tuned using collection policies. Easy **deployment** to the whole network such as using AD, SCCM or psexec.

Integration with SIEM, VDI, LDAP, AD, 2-fact Authen, APIs. Sensor Emergency & Autoupdate. Server: Multisite and audited.

Contact: Lan Nguyen, PhD. Co-founder & EVP. Email: lan@veramine.com