Folders created by the malware

Malicious attachments

Malware modules installed in the system

Legitimate objects used by the malware

Malware configuration files

Malware registry keys

Typical characteristics of the network activity of legitimate software used by the attackers

1. Host: server.remoteutilities.com
2. Host: rmansys.ru
3. Host: rms-server.tektonit.ru
4. User-Agent: Mozilla/4.0 (compatible; RMS)
5. User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
6. Connections to servers *.teamviewer.com
7. A combination of the following fields in HTTP headers: HTTP/1.0 and Content-Type: image/jpeg.

Servers used by the attackers

The web resources listed below are not associated with any real-world organizations; the attackers chose some of the domain names to disguise their resources as the resources of well-known companies.

t x s s wxyprz
t p
st r x x x s p xrx ux t ts x P
wp w p tup s up p s
wp w t t t t p uu ut u u u
t x
x v
p p s ruv u s
p p s ruv xst u s
x s u s
zx xst u s
r sx x
x P S
p s p u p
p s p u
p s ux t x t

t tp xt t x v s wxyprz
t p
st r x x x v s p xrx ux t ts x tp xt t
wp w t usu s u u u s t s
wp w r t s ss u p
t x

x v
p x v s u s

r sx x
x P S
p s p u p
p s t t r px
p s t t u t
p s ux t x t
p s ux t x t