Table 4: A complete description of the set of features used in this study.

Feature	class	sub-class	description
fc	file system	file operation	Count of files created
fm	file system	file operation	Count of files modified
fd	file system	file operation	Count of files deleted
sz1	file system	file size	Count of normalized file sizes created that are less than 25% of the files created
sz2	file system	file size	Count of normalized file sizes created that are less than 50% and more then 25%
sz3	file system	file size	Count of normalized file sizes created that are less than 75% and more then 50%
sz4	file system	file size	Count of normalized file sizes created that are more than 75% of the files created
nue	file system	file extension	Count of unique extensions
au	file system	file path	Count of files created under ALLUSERPROFILE path
ad	file system	file path	Count of files created under APPDATA path
cp	file system	file path	Count of files created under COMMONPROGRAMFILES path
pf	file system	file path	Count of files created under PROGRAMFILES path
wd	file system	file path	Count of files created under WINDIR path
up	file system	file path	Count of files created under USERPROFILE path
tm	file system	file path	Count of files created under TEMP path
rc	registry	key operation	Count of created registry keys
rm	registry	key operation	Count of modified registry keys
rd	registry	key operation	Count of deleted registry keys
rs	registry	key type	Count of registry keys with REG_SZ type
rb	registry	key type	Count of registry keys with REG_BINARY type
rw	registry	key type	Count of registry keys with REG_DWORD type
ipn	network	IP address	Count of unique destination IPs
p0	network	port number	Count of connections to port 20
p1	network	port number	Count of connections to port 21
p2	network	port number	Count of connections to port 22
p3	network	port number	Count of connections to port 25
p4	network	port number	Count of connections to port 53
p5	network	port number	Count of connections to port 80
p6	network	port number	Count of connections to port 102
p7	network	port number	Count of connections to port 110
p8	network	port number	Count of connections to port 143
p9	network	port number	Count of connections to port 389
p10	network	port number	Count of connections to port 443
p11	network	port number	Count of connections to port 465
p12	network	port number	Count of connections to port 587
p13	network	port number	Count of connections to port 636
p14	network	port number	Count of connections to port 993
p15	network	port number	Count of connections to port 995
p16	network	port number	Count of connections to port 6347 to 6665 or 6679, 6697 (IRC)
p17	network	port number	Count of connections to port 8080
p18	network	port number	Count of connections to other unaccounted for ports
tcp	network	connection type	Count of TCP connections
udp	network	connection type	Count of UDP connections
raw	network	connection type	Count or RAW connections
rz1	network	request size	Count of the normalized network request size less than 25%
rz2	network	request size	Count of the normalized network request size less than 50% greater than 25%
rz3	network	request size	Count of the normalized network request size less than 75% greater than 50%
rz4	network	request size	Count of the normalized network request size greater than 75%
pst	network	request type	Count of POST requests
get	network	request type	Count of GET requests
hed	network	request type	Count of HEAD requests
th	network	response type	Count of response code 200s
thh	network	response type	Count of response code 300s
fh	network	response type	Count of response code 400s
fvh	network	response type	Count of response code 500s
hz1	network	response size	Count of the normalized reply size less than 25%
hz2	network	response size	Count of the normalized reply size less than 50% greater than 25%
hz3	network	response size	Count of the normalized reply size less than 75% greater than 50%
hz4	network	response size	Count of the normalized reply size greater than 75%
mx	network	DNS type	Count of DNS MX
ns	network	DNS type	Count of DNS NS
a	network	DNS type	Count of DNS A
ptr	network	DNS type	Count of DNS PTR
soa	network	DNS type	Count of DNS SOA
cn	network	DNS type	Count of DNS CNAME