1) crontab ima sljedeću sintaksu: " * * * * * path/to/command" i služi za izvršavanje komandi u određeno vrijeme, koje se navodi na pozicije zvjezdica (minuta, sat, dan, mjesec, dan u tjednu). Ako napadač zna da postoji: " */5 * * * * /usr/local/bin/backup" tada zaključuje da se skripta backup pokreće svake pete minute u svakom satu (periodičan poziv se dobije ako se stavi kosa crta ispred broja).
Čitanjem sadržaja skripte backup pomoću naredbe cat doznajemo da je skripta napisana u jeziku bash i da poziva drugu skriptu s lokacije /tmp/smth (ako ona postoji) i to čini pozivom naredbe za čitanje i izvršavanje "source /tmp/smth".
Potrebno je kreirati zlonamjernu skriptu za dodjelu administrativnih ovlasti korisniku sui koju je potrebno pozicionirati na mjesto /tmp/smth, to činimo naredbom: "echo 'sudo usermod -a -G sudo sui' > /tmp/smth" i čekamo maksimalno pet minuta da se skripta pozove nakon čega restartamo virtualni stroj. Pozivom naredbe "sudo cat /etc/sudoers" pronalazimo liniju koja omogućava korisnicima grupe sudo da izvršavaju naredbe s pravima root korisnika: "%sudo ALL=(ALL:ALL) ALL "

2) Dodavanje novog korisnika u operacijski sustav moguće je učiniti pozivom naredbe: "sudo adduser jakov". Redci u /etc/passwd datoteci imaju sljedeća polja odvojena dvotočkom:

Username	Korisničko ime (root, sui, jakov, ...)
Password	Ako je prisutan "x" znači da postoji šifrirana lozinka u /etc/shadow datoteci
User ID (UID)	Korisnički ID (0 je za root, 1-99 su rezervirani)
Group ID (GID)	Primarni ID grupe (pohranjena u /etc/group datoteci)
User ID info	Korisničke informacije (ime i prezime, broj mobitela, ...)
Home directory	Path do direktorija u kojemu će se korisnik nalaziti nakon prijave
Command/shell	Path do ljuske korisnika

Redci u /etc /shadow datoteci imaju sljedeća polja odvojena dvotočkom:

Username	Korisničko ime (root, sui, jakov, ...)
Password	Format: idsalt$hashed gdje $id označava vrstu hash algoritma
Last password change	Broj proteklih dana = 1.1.1970 - današnji datum
Minimum	Minimalan broj dana koji moraju proći za promjenu lozinke
Maximum	Maksimalan broj dana koji moraju proći za promjenu lozinke
Warn	Koliko dana prije isteka lozinke da se korisnik upozori na istek
Inactive	Koliko dana nakon isteka lozinke je račun onemogućen
Expire	Koliko dana od 1.1.1970 otkad je račun onemogućen

Možemo vidjeti da redci za korisnika jakov i sui nisu isti iako im je lozinka jednaka. Razlog tome je što se koristi različiti SALT (dodatni nasumični bitovi koji se konkateniraju lozinci prije poziva hash funkcije). Hash funkcija koja se koristi je SHA-512.
Pozivom naredbe "mkpasswd -m sha-512 -S fQpJALep Internet1" možemo generirati hash za proizvoljnu lozinku i proizvoljan SALT.

3) Kako bi usporedili brzine pronalaženja lozinki potrebno je u rječnik password.lst nadodati lozinku "rockyou" jer je za pronalazak svih 100 lozinki algoritma SHA-256 bilo potrebno više od 3h. Naredba koju pozivamo je " sudo sh -c "echo 'rockyou' >> /usr/share/john/password.lst" "

MD5	0:00:00:12
SHA-256	0:00:08:11

SHA-256_weak	0:00:00:29
SHA-512	0:00:07:17
SHA-512_weak	0:00:00:22

Datoteke koje imaju dodatnu oznaku weak, imaju isti SALT ("SigurnostIntSALT") za svaku od 100 lozinki. Alat John The Ripper radi sa "Single crack" načinom rada koji je najbrži, također može raditi s rječnikom kojeg mu napadač priloži i može raditi sa "Incremental" načinom rada koji testira svaku moguću kombinaciju slova i brojki.

4) Kada korisnik pokrene izvršnu datoteku malware1 instalirat će mu se program u web-server direktorij, koji će omogućiti napadaču da se spoji na računalo korisnika i to preko Interneta putem HTTP protokola. Napadač može pokrenuti razne naredbe na računalu korisnika bez njegovog dopuštenja. Neke od tih naredbi su kreiranje novog root korisnika ili isključivanje računala... Riječ je o rootkit zlućudnom programu.

Ako korisnik pokrene izvršnu datoteku malware2 uzrokovat će si DoS (Denial-of-Service) napad na mreži i bit će mu onemogućen pristup Internetu. Također, zlućudni program će se samo umnožiti i poslati dalje e-mailom. Riječ je o crvu.

Usporedbom zaključujemo da prvi alat se služi otvaranju backdoora u sustav i da tako preuzima neovlašteni nadzor nad računalom. Drugi alat umnaža samog sebe tako da se šalje e-mailom dalje i radi Denial-of-Service nad TCP i UDP paketima.